UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Materiales de apoyo para Seguridad Informática Básica

MATERIAL DIDÁCTICO

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Nanci Noelia Granados Gómez

ASESORA DE MATERIAL DIDÁCTICO

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2024

Agradecimientos y dedicatorias

Desde pequeña había soñado con culminar mis estudios, ahora esto es una realidad, y durante el proceso estuvieron involucradas una gran cantidad de personas por lo que me es difícil agradecer particularmente a cada una.

Primeramente, quiero agradecer a mis padres por haberme apoyado en cada paso y en cada momento, por haberme alentado a perseguir mis sueños y por enseñarme a no darme por vencida, entre otras muchas cosas, gracias a ustedes he podido alcanzar mis objetivos personales, escolares y profesionales.

A mis amigos, quienes me acompañaron a lo largo de este camino, con quienes más que compartir clases, compartí momentos, y aprendí de ellos que una buena amistad, aunque sea ausente, está a tu lado en todo momento.

A mi asesora, quien durante el desarrollo de este proyecto estuvo dispuesta a orientarme, ayudarme y corregirme, por su paciencia y dedicación a este proyecto.

A mis profesores quienes con sus enseñanzas me ayudaron a crecer, y que, aunque en este momento algunos ya no estén físicamente aquí siempre los tendré presentes, ya que, con sus enseñanzas alimentaron mis ganas de seguir aprendiendo.

A mi casa de estudios, por permitirme formar parte de una gran institución como lo es la UNAM, porque desde mi ingreso al Colegio de Ciencias y Humanidades plantel Oriente hasta mi egreso de la Facultad de Ingeniería me brindó las herramientas necesarias para poder culminar mis estudios, además de darme la oportunidad de conocer a compañeros amigos y maestros de quienes aprendí en cada momento compartido.

Introducción

Actualmente, la tecnología está involucrada en muchos aspectos de nuestra vida cotidiana, lo cual trae consigo muchas ventajas, ya que, desde diferentes dispositivos se puede tener acceso a información y herramientas almacenadas en internet, asimismo, la tecnología puede ser útil para otras cosas más, entre ellas, aumentar la productividad con la automatización de tareas o acceder a información a través de los diferentes buscadores de internet, lo cual es muy útil para adquirir conocimiento de diferentes temas, también la tecnología ofrece entretenimiento, como videojuegos, contenido multimedia o acceso a redes sociales.

Como se puede observar, las ventajas del uso de la tecnología son muy amplias, pero también tiene su contraparte, pues tener acceso a diferentes aplicaciones, plataformas o dispositivos de tecnología conlleva diferentes desventajas, entre las cuales se pueden encontrar desde dependencia a los dispositivos de tecnología por parte de los usuarios, hasta dilemas éticos, riesgos de seguridad e incluso contaminación ambiental.

De acuerdo con el Índice de Ciberseguridad Global (ICG), México se encuentra entre los países con mayores vulnerabilidades cibernéticas, organizaciones y empresas son amenazadas por ciberdelincuentes, quienes atacan su infraestructura o causan daños de manera lógica en sus redes, comprometiendo tanto su red interna como externa, lo que causa problemas en su productividad, ya que este tipo de amenazas afecta a los usuarios internos y externos. (Infobae México, 2023)

Por lo anterior, es que se vuelve indispensable el estudio de la seguridad informática por parte de los profesionales. La asignatura de Seguridad Informática Básica incluida en el plan de estudios de la carrera de Ingeniería en Computación impartida en la Facultad de Ingeniería tiene un papel muy importante en la formación de profesionales, esto se debe a que desde hace algunos años la humanidad ha vivido en un mundo digital, donde la protección de la información ha sido una tarea sumamente importante.

Teniendo como referencia datos recopilados por el laboratorio de inteligencia de amenazas FortiGuard, en el primer semestre del año 2022, México ha sido el país de América Latina que más intentos de ciberataques ha recibido, registrando más de 85,000 millones de intentos de ciberataques, donde la estrategia más usada ha sido el uso de ransomware, registrando más de 18.000 detecciones de distribución. (eSemanal, 2022)

En la encuesta Digital Trust Insights del año 2024 realizada por PwC, también conocida como PriceWaterhouseCoopers, dio a conocer que en México las empresas se sienten mejor preparadas para hacer frente a los ciberdelincuentes, esto incluye capacitar y concientizar a los empleados que pertenecen a áreas diferentes a las de ciberseguridad, además, destaca que las amenazas más preocupantes para el 2024 son el filtrado de información, hackeos, amenazas a la nube y ataques a dispositivos de IoT (Internet of Things o Internet de las cosas). (PricewaterhouseCoopers, s. f.)

Es indispensable tener profesionales capacitados para enfrentar a grupos de ciberdelincuentes y brindar soluciones de seguridad, con el objetivo de proteger la información e infraestructura de alguna empresa u organización de las diferentes formas de ataques que se viven actualmente, es por ello que la Facultad de Ingeniería se compromete a preparar a sus estudiantes en estas áreas con el fin de que adquieran las capacidades necesarias para afrontar los retos presentes y futuros en el campo de la seguridad informática.

Adicionalmente, derivado de los semestres impartidos en línea a causa de la pandemia por COVID – 19 se detectó la falta de materiales complementarios para la asignatura antes mencionada, a raíz de esta problemática surge la propuesta de desarrollarlos con el fin de que sean de utilidad tanto para estudiantes como para el personal académico.

Con base en lo antes mencionado, es que el objetivo del presente trabajo es desarrollar materiales de clase complementarios para estudiantes y docentes de la carrera de Ingeniería en Computación de la Facultad de Ingeniería, para la asignatura de Seguridad Informática Básica, el cual se compone de 3 partes:

- Investigación documental del temario de la asignatura.
- Material audiovisual de cada tema.
- Reactivos por cada tema.

Referente a la investigación documental, se hizo un compilado de información de distintas fuentes confiables, como artículos, datos del INEGI, libros, tesis, entre otros, además, la coordinadora del área de redes y seguridad de la Facultad de Ingeniería de la UNAM, quien es la asesora de este trabajo revisó puntualmente la información con el fin de garantizar y brindar más confiabilidad a la información.

El objetivo principal de la investigación documental es que el alumnado tenga una fuente confiable de información de acuerdo con el temario de la asignatura y el personal docente cuente con materiales de apoyo para impartir dicha materia.

Para lograr esto, es que cada uno de los capítulos pretende explicar desde conceptos básicos hasta algunas de las diferentes formas de ataque llevadas a cabo por ciberdelincuentes, así como explicar algunos de los estándares importantes para llevar a cabo esta labor, incluyendo la ética informática y el impacto económico y social que tiene la seguridad informática actualmente.

Posteriormente, dicha investigación fue complementada realizando materiales audiovisuales, con los cuales se pretende tener un resumen de los temas más relevantes desarrollados, cuyo objetivo es permitir que el estudio se vuelva más ágil.

Además, es importante destacar que se realizó una serie de reactivos por cada tema, a fin de que el estudiantado tenga la oportunidad de revisar sus avances en el aprendizaje de la asignatura, teniendo 274 reactivos repartidos entre los seis temas que componen el temario.

Finalmente, los materiales de estudio, el material audiovisual y los reactivos fueron colocados en la plataforma Moodle, propia del área de redes y seguridad, a la cual tendrán acceso alumnos y profesores, por lo que podrán consultar la información en el momento que lo necesiten.

Índice de contenido

Índice de figuras

Índice de tablas

Tema 1. Fundamentos teóricos

1.1 Introducción

1.1.1 Concepto de la seguridad informática

Actualmente vivimos en un mundo donde la tecnología juega un papel muy importante, volviéndose un tema de interés público, por lo que es muy importante entender este concepto.

La seguridad informática puede ser definida como un conjunto de medidas las cuales sirven para evitar que se ejecuten acciones no autorizadas en los sistemas informáticos, esto porque pueden provocar diferentes daños, entre ellos, comprometer la integridad, confidencialidad o autenticidad de los sistemas o de la información que contienen. También puede verse como un proceso donde se definen las técnicas, prácticas y procedimientos para prevenir daños o alteraciones a los recursos informáticos, garantizando así su correcto funcionamiento.

Teniendo estas definiciones en cuenta, se puede decir que la seguridad informática es un proceso que consiste en prevenir el acceso no autorizado a los sistemas informáticos, con la finalidad de prevenir alteraciones y/o modificaciones a dicho sistema, para que los recursos funcionen de manera adecuada, preservando así la confidencialidad, integridad y disponibilidad o mejor conocido como triangulo CID, que se revisará a detalle más adelante.

Para hacer seguridad informática hay algo conocido como “principio de defensa en profundidad”, el cual, a grandes rasgos, consiste en diseñar diferentes niveles se seguridad en los sistemas informáticos, el cual se explicará a profundidad más adelante.

Llegando a este punto se tiene que tomar en cuenta otro concepto, el cual es “seguridad de la información”, ya que muchas veces suele ser confundido con el concepto se seguridad informática.

La seguridad de la información son medidas que protegen los activos informáticos, hay que recordar que los activos informáticos son los recursos que tienen valor para una organización, siendo la información su activo más importante, por lo que la seguridad de la información se encargará de proteger los activos informáticos de las organizaciones.

Por otro lado, la seguridad informática puede verse como un conjunto de técnicas que ayudarán a proteger los sistemas informáticos, donde ya se ve involucrada la infraestructura.

Como se puede observar, son conceptos diferentes, que a menudo suelen ser confundidos.

(Calderón Arateco, s. f.; López Barrientos & Quezada Reyes, 2019; Moreno López, s. f.; Rentería Echeverry, s. f.; Romero Castro et al., 2018)

1.1.2 Evolución histórica de la seguridad informática

Desde hace varias décadas, surge la necesidad de proteger los sistemas informáticos. Con el aumento del uso de la tecnología surge la necesidad de proteger los sistemas informáticos de accesos no autorizados, mencionado esto, iniciemos en la década de 1960.

- **Inicios de 1960:** en los inicios de esta década no existía el internet, por lo que la seguridad de los sistemas informáticos se enfocaba en la seguridad física de dichos sistemas, por lo que las organizaciones comenzaron a tomar medidas para proteger los equipos con los que contaban, esto lo hacían mediante el uso de contraseñas en los dispositivos esto para garantizar la protección de la información que contenían.
  Es también en esta década donde surge la Agencia de Proyectos de Investigación Avanzada, mejor conocida como ARPA por sus siglas en inglés Advanced Research Projects Agency, cuyo objetivo era crear una red de computadoras.
- **1962:** ARPA creó un programa de investigación computacional, dirigido por John Licklider. Al mismo tiempo, Leonard Kleinrock, Donald Davies y Paul Baran quienes eran investigadores, buscaban una forma segura de comunicación, por lo que realizaron las investigaciones de forma paralela, lo que nos lleva a dar un brinco hasta el año 1968.
- **1968:** es en este año, cuando ARPA hace uso de los tres proyectos anteriores para la implementación de una red de computadoras que comunicara instituciones académicas y estatales, por lo que surge el plan para la construcción de lo que llamaron ARPANET o Advanced Research Projects Agency Network, que en español significa Red de Agencias de Proyectos de Investigación Avanzada.
- **29 de octubre de 1969:** este día es cuando se realiza la primera comunicación a través de ARPANET, entre la UCLA (University of California at Los Angeles o en español Universidad de California en los Ángeles), y el SRI (Stanford Research Institute o Instituto de Investigación de Stanford), esta comunicación consistía en enviar un mensaje cuyo contenido era una palabra: “login”, sin embargo, solo se pudieron enviar las primeras dos letras antes de que se perdiera la conexión, una hora después se pudo realizar el envió completo del mensaje. Fue hasta el 21 de noviembre del mismo año cuando se logró establecer una conexión permanente entre la UCLA y el SRI, y el 5 de diciembre del mismo año se logó establecer una conexión permanente entre los cuatro nodos iniciales, dando así por sentadas las bases que actualmente se conocen como internet. (NIC Argentina, 2017)

Nota:

Antes del surgimiento del ARPANET, la forma de comunicarse era mediante el telégrafo, por lo que se tienen el registro del primer hacker de la historia, quien fue el mago Nevil Maskelyne, quien logró interceptar el telégrafo inalámbrico en el año de 1903.

El primer ciberdelincuente del que se tiene registro es John Draper, quien descubrió que podía realizar llamadas gratis, modificando el silbato de las cajas de cereal Cap’n Crunch para engañar a la central telefónica.

Para continuar con la evolución historia de la seguridad informática, se tiene que tomar en cuenta que con el surgimiento de ARPANET surge la necesidad de proteger la información que viajaba por esta red de computadoras, por lo que iremos a la década de 1970.

- **Década de 1970:** Bob Thomas creó un programa que podía moverse por ARPANET, este programa fue llamado CREEPER y es considerado el primer virus. Este virus dejaba un rastro por donde pasaba, el cual era un mensaje impreso que decía: “I’m the creeper: catch me if you can”.
  Poco tiempo después, Ray Tomlinson diseñó un programa que se autorreplicaba, convirtiéndose así en el primer gusano informático. Después surge REAPER, este también era un virus que buscaba en la red el rastro de CREEPER para eliminarlo, surgiendo así el inicio de los antivirus.
- **1980:** James P Anderson escribió el documento “Computer Security Threat Monitoring and Surveillance”, donde sentó los pilares de la seguridad informática, y es así como las organizaciones implementan software para proteger sus sistemas informáticos.
- **1980 – 1990: Serie arcoíris:** la serie arcoíris (véase la figura 1.1) es un conjunto de estándares de seguridad informática que describen un proceso de evaluación de sistemas confiables los cuales fueron publicados por el gobierno de Estados Unidos, originalmente por el Centro de Seguridad Informática del Departamento de Defensa de EE.UU y posteriormente por el Centro Nacional de Seguridad Informática.
  El nombre “serie arcoíris” deriva de los colores de las portadas de los libros y cada uno de ellos es más conocido por el color de su portada. Esta serie aun es usada como estándar en contratos gubernamentales.

Figura 1.1. Serie arcoíris.

[Fotografía] (2022, 18 diciembre), Intrinsically Secure. https://www.linkedin.com/pulse/intrinsically-secure-mark-winstead?trk=pulse-article_more-articles_related-content-card

Los libros más importantes de la serie arcoíris son:

Tabla 1.1. Libros de la serie arcoíris.

Documento	*Título*	Fecha de publicación	Color
Serie arcoíris del Departamento de Defensa			
CSC-STD-001-83	*Criterios de evaluación del sistema informático de confianza del DOD*	15/08/1983	Naranja
CSC-STD-002-85	*Pautas de administración de contraseñas del DOD*	12/041985	Verde
CSC-STD-003-85	*Orientación para la aplicación de TCSEC en entornos específicos*	25/06/1985	Amarillo claro
CSC-STD-004-85	*Justificación técnica de CSC-STD-003-85: Requisitos de seguridad informática*	25/06/1985	Amarillo II
Serie arcoíris NSA/NCSC			
NCSC-TG-001	*Una guía para comprender la auditoría en sistemas confiables*	01/06/1988	Marrón
NCSC-TG-002	*Programa de evaluación de seguridad de productos de confianza*	22/06/1990	Azul brillante
NCSC-TG-003	*Control de acceso discrecional en sistemas confiables*	30/09/1987	Naranja neón
NCSC-TG-004	*Glosario de términos de seguridad informática*	21/10/1988	Verde azulado
NCSC-TG-005	*Interpretación de la red de confianza*	31/07/1987	Rojo
NCSC-TG-006	*Gestión de la configuración en sistemas fiables*	28/03/1988	Ámbar
NCSC-TG-007	*Una guía para comprender la documentación de diseño en sistemas confiables*	06/10/1988	Borgoña
NCSC-TG-008	*Una guía para comprender la distribución confiable en sistemas confiables*	15/12/1988	Lavanda
NCSC-TG-009	*Interpretación del subsistema de seguridad informática del TCSEC*	16/09/1988	Azul Venecia
NCSC-TG-010	*Una guía para comprender el modelado de seguridad en sistemas confiables*	Octubre 1992	Agua
NCSC-TG-011	*Pauta de entornos de interpretación de redes confiables (TNI)*	01/08/1990	rojo
NCSC-TG-012	*Interpretación del sistema de gestión de bases de datos de confianza* [3]	Abril 1991	
NCSC-TG-013	*Documento de programa RAMP*	1989	Rosa
NCSC-TG-013 V2	*Documento de programa RAMP versión 2*	01/03/1995	Rosa
NCSC-TG-014	*Directrices para sistemas formales de verificación*	01/04/1989	Púrpura
NCSC-TG-015	*Guía para comprender la administración de instalaciones confiables*	18/101989	Marrón
NCSC-TG-016	*Directrices para la redacción de manuales de instalaciones de confianza*	Octubre 1992	Amarillo verde
NCSC-TG-017	*Identificación y autenticación en sistemas confiables*	Septiembre 1991	Azul claro
NCSC-TG-018	*Reutilización de objetos en sistemas confiables*	Julio 1992	Azul claro
NCSC-TG-019	*Cuestionario de evaluación de productos de confianza*	02/05/1992	Azul
NCSC-TG-020	*Trusted UNIX Working Group (TRUSIX) Justificación para seleccionar funciones de lista de control de acceso para el sistema UNIX*	7/07/1989	Plata
NCSC-TG-020-A	*Trusted UNIX Working Group (TRUSIX) Justificación para seleccionar funciones de lista de control de acceso para el sistema UNIX (R)*	18/08/1989	Gris plata
NCSC-TG-021	*Interpretación del sistema de gestión de bases de datos fiables del TCSEC (TDI)*	Abril 1991	Púrpura
NCSC-TG-022	*Recuperación confiable en sistemas confiables*	30/12/1991	Amarillo
NCSC-TG-025	*Guía para comprender la remanencia de datos en sistemas de información automatizados.*	Septiembre 1991	Bosque verde
NCSC-TG-026	*Redacción de la guía del usuario de funciones de seguridad para sistemas de confianza*	Septiembre 1991	Melocotón
NCSC-TG-027	*Responsabilidades del oficial de seguridad del sistema de información para los sistemas de información automatizados*	Mayo 1992	Turquesa
NCSC-TG-028	*Evaluación de la protección de acceso controlado*	25/05/1992	Violeta
NCSC-TG-029	*Conceptos de certificación y acreditación*	Enero 1994	Azul
NCSC-TG-030	*Análisis de canal encubierto de sistemas confiables*	Noviembre 1993	Rosa claro

Tabla tomada de: https://hmong.es/wiki/Rainbow_Series

Corregida y revisada con: https://irp.fas.org/nsa/rainbow.htm

- **1983:** Surge el *"libro naranja",* fue desarrollado por el DOD, Department of Defense o Departamento de Defensa, este libro muestra requerimientos básicos de seguridad que una organización debe aplicar para mantener seguro un sistema, con el fin de proteger la confidencialidad de la información. El contenido de este libro será explicado con un poco de detalle en el subtema de normatividad.
- **1991:** Francia, Alemania, Los Países Bajos y el Reino Unido publicaron el Information Technology Security Evaluation Criteria por sus siglas en inglés ITSEC, en español conocido como Criterios de Evaluación de Seguridad en Tecnologías de la Información, los criterios que contiene están divididos en niveles de evaluación que van de E0 a E6, los cuales representan un nivel de confianza para alcanzar un objetivo de seguridad. Este conjunto de criterios tiene un enfoque más amplio que su antecesor, el Trusted Computer System Evaluation Criteria, por sus siglas en ingles TCSEC, en español conocido como Criterios de Evaluacióndel Sistema Informático de Confianza, o libro naranja.
- **1993:** Los países que publicaron el ITSEC, con el apoyo de SOGIS que en inglés significa Senior Officials Group Information Systems Security, traducido al español como Grupo de Altos Funcionarios de Seguridad de los Sistemas de Información, produjeron un borrador de una metodología que complementaría los criterios del ITSEC, al cual llamaron ITSEM (Information Technology Security Evaluation Manual o Manual de Evaluación de la Seguridad de las Tecnologías de la Información). ITSEC e ITSEM en conjunto están orientados a la evaluación técnica de productos y sistemas, sin cubrir medidas administrativas, organizativas o de personal que no estuvieran relacionadas con las TI.
- **1993:** Canadá publica el Canadian Trusted Computer Product Evaluation Criteria por sus siglas en inglés CTCPEC, conocido en español como Criterios de Evaluación de Productos Informáticos de Confianza de Canadá, este conjunto de criterios es una combinación de los criterios americanos y europeos. El CTCPEC verifica que el producto esté implementado correctamente, teniendo como base las políticas de seguridad establecidas.
- **1995:** surge la norma BS 7799-1, ésta es un conjunto de buenas prácticas las cuales ayudaban a las empresas con la administración de la seguridad de la información.
- **1996:** surge la versión 1.0 de los Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información, también conocidos como Common Criteria o CC, estos fueron el resultado final del desarrollo de los criterios de evaluación elaborados anteriormente, evalúan la seguridad de los productos de TI y surgieron como resultado de la concientización sobre la seguridad informática por parte del gobierno de Estados Unidos.
- **1998:** surge la norma BS 7799-2, esta segunda versión de la norma de 1995 tuvo muchas mejoras por lo que la ISO o International Organization for Standardization, conocida en

español como Organización Internacional de Normalización, comenzó a hacer una revisión de todos los cambios.

- **2000:** la ISO toma la norma BS7799-1 y la publica con el nombre de ISO 177991, esta no incluye la segunda parte de la norma publicada en 1998.
- **2002:** se publica una nueva versión de la norma BS 7799-2, en esta nueva versión se permite la acreditación de empresas por parte de una entidad certificadora en Reino Unido y otros países.
- **2005:** el 15 de octubre de 2005, la norma BS 7799-2 se publicó como el estándar ISO 27001, convirtiéndose en la norma principal de la serie 27000, la cual contiene los requisitos del Sistema de Gestión de Seguridad de la Información o SGSI, es decir, contiene medidas de seguridad que protegen la información de cualquier amenaza, independientemente del formato en el que se encuentre. Al mismo tiempo se hizo una revisión y actualización de la norma ISO 17799.
- **2007:** el 1 de julio de 2007, la norma ISO 17799 es renombrada como ISO 27002, manteniendo su contenido y el año de publicación formal de la revisión.

(Alonso, 2015; Castillo Maza, 2003; Grupo ESGinnova, 2013; Iriarte Medina, 2006; Murphey, 2019)

1.1.3 Objetivos de la seguridad informática

Desde el año 1988 se declaró el 30 de noviembre como el “Día internacional de la seguridad informática”, esto tiene como objetivo hacer conciencia sobre la importancia que tiene la seguridad de los sistemas, para preservar la información que estos contienen.

Los principales objetivos que debe cumplir la seguridad informática son los siguientes:

- Disponibilidad.
- Confidencialidad.
- Integridad.
- No repudio.
- Autenticación.
- Control de acceso.

Este conjunto de objetivos es conocido como *servicios de seguridad,* estos son muy importantes para proteger de manera adecuada los sistemas informáticos junto con la información que estos almacenen.

Es importante proteger todos los sistemas, no solo aquellos que se encuentren conectados a una red, ya que podría haber un caso en donde el sistema se encuentre aislado pero la información que contiene puede estar almacenada en un servidor que sí se encuentre en una red, y si no se protege correctamente el sistema podría estar en riesgo.

Aunado a esto, se tiene que la seguridad informática ayuda a minimizar los riesgos y detectar amenazas de seguridad para así evitar que la información se pierda por completo en caso de algún incidente, y que en el caso de que el sistema sea vulnerado se tenga la menor pérdida de información posible. Además, ayuda a que los recursos sean aprovechados de forma efectiva y estos funcionen correctamente.

Para poder cumplir los objetivos, las organizaciones deben de contemplar cuatro planos:

- **Técnico:** a nivel físico y nivel lógico.
- **Legal:** esto se debe a que en algunos países se tiene que cumplir con un conjunto de medidas de seguridad en algunos sectores.
- **Humano:** capacitar a los empleados, definir las funciones y obligaciones del personal.
- **Organizativo:** tener un protocolo para actuar ante cualquier tipo de incidente, tener políticas de seguridad adecuadas, así como un conjunto de normas y procedimientos que ayuden a cubrir las necesidades de la organización.

(Delgado Avenia, 2017; López Barrientos & Quezada Reyes, 2019)

1.1.3.1 Ciclo de la seguridad informática

Puede entenderse como ciclo a un periodo de tiempo durante el cual suceden una serie de fenómenos o etapas en cierto orden, que una vez finalizadas vuelven a repetirse una y otra vez.

Teniendo como base lo anterior, la seguridad informática cuenta con una serie de fases, con las cuales se pueden llegar a determinar riesgos o vulnerabilidades, y en donde cada una de las amenazas detectadas tengan un tratamiento para eliminarlo, al mismo tiempo que se busca evitar que se vuelva a repetir.

Por más que se crea que un sistema se encuentra protegido, se debe recordar que nada impide que ocurra un incidente por lo que es importante aplicar medidas de seguridad, que sean tanto correctivas como preventivas, teniendo en cuenta que siempre es mejor prevenir los incidentes que corregirlos.

El ciclo de la seguridad informática debe mantenerse dentro de una organización, ya que cada una de las fases que lo conforman sirve para mitigar los riesgos o amenazas que puedan presentarse. Las fases de este ciclo se presentan a continuación:

- **Evaluación:** es necesario saber en qué estado se encuentra la seguridad del sistema, durante la evaluación se debe de determinar el entorno en el que se basa la organización, así como el núcleo de la misma, con el objetivo de analizar las vulnerabilidades que se encuentren, además esto ayuda a tener un mejor conocimiento del sistema y así crear conciencia sobre el estado en el que éste se encuentre.

- **Diseño:** después de que el sistema fue evaluado, hay que diseñar soluciones para mitigar las vulnerabilidades que se hayan encontrado, así mismo deben de tenerse parámetros que sirvan de referencia para indicar que si ha tenido o no éxito.
- **Implementar:** esta fase es la encargada de implementar las soluciones diseñadas en la fase anterior, todo debe de ser documentado, incluidos los problemas encontrados, así como las soluciones implementadas. También hay que comparar los resultados obtenidos con los parámetros de éxito establecidos.
- **Administración y soporte:** esta fase es la encargada de generar mejoras continuas de todo el proceso, por lo que se tiene que seguir monitoreando todo el sistema para saber el estado en el que se encuentre y documentar las nuevas vulnerabilidades que se vayan encontrando.

Cómo se puede observar, para que la seguridad informática cumpla sus objetivos debe de funcionar de acuerdo a un ciclo, por lo que al aplicar medidas de seguridad no se puede dar por sentado que el sistema se encontrará completamente seguro, por lo que es necesario mantener actualizadas las medidas aplicadas al sistema para evitar en mayor medida la ocurrencia de incidentes, y en dado caso que se produzca un incidente, analizarlo para saber cómo y porqué fue que ocurrió, para así diseñar la solución respectiva y que éste no se vuelva a repetir.

Como se observa, en este tema se mencionaron los riesgos, los cuales se deben tener presentes ya que un riesgo de seguridad es cuando una vulnerabilidad es explotada y ésta genera pérdidas, lo que afecta directamente el funcionamiento de la organización. El tema de riesgos es muy importante, por lo que más adelante se estudiará a profundidad.

(Delgado Avenia, 2017; Iriarte Medina, 2006; López Barrientos & Quezada Reyes, 2019; Rentería Echeverry, s. f.)

1.1.4 Principio de profundidad – principio de defensa en profundidad

Este concepto tiene un origen etimológico en el mundo militar. La defensa en profundidad es una estrategia que se usa para evitar que un enemigo avance rápidamente, así al retrasar el avance, el enemigo pierde fuerza e impulso, proporcionando tiempo adicional para elaborar una respuesta efectiva.

De acuerdo con el CIS Center of Internet Security o Centro de Seguridad en Internet, el principio de defensa en profundidad pretende implementar un conjunto de mecanismos que protejan la integridad, confidencialidad y disponibilidad de la red y los datos que contiene. Es imposible que alguna tecnología o control sea capaz de contener todas las amenazas y ataques, sin embargo, dentro del conjunto de mecanismos implementado se puede brindar una mayor protección

contra las amenazas, además de brindar redundancia en caso de que algún mecanismo en particular falle.

Como ya se mencionó, el objetivo principal del principio de defensa en profundidad es buscar métodos que disminuyan la probabilidad de que un sistema sea vulnerado, esto lo hace implementando seguridad a cada una de las capas del sistema, lo que aumenta la posibilidad de identificar atacantes a tiempo para así evitar que exploten las vulnerabilidades que el sistema pueda tener.

Las capas de este principio pueden observarse en la figura 1.2:

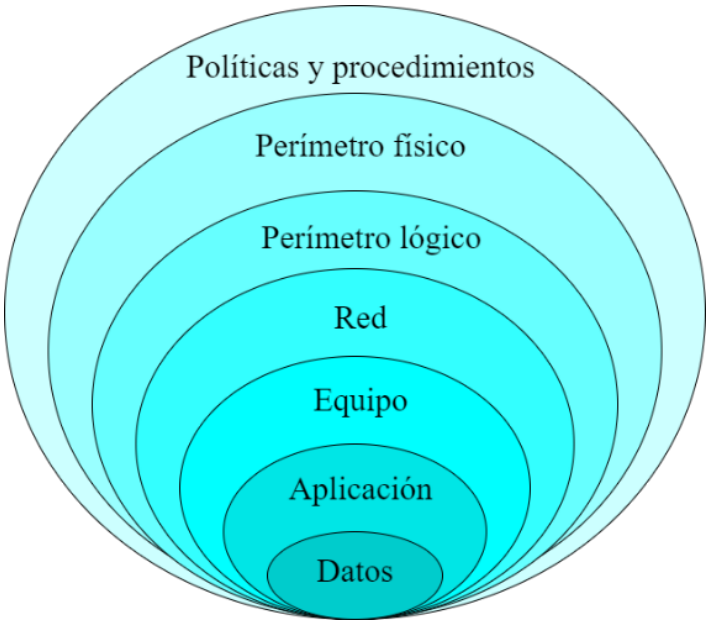


Figura 1.2. Capas del principio de profundidad.

Como se vio al inicio del tema, el activo más importante que una organización debe proteger son los datos, es por ello que se encuentra en la capa más profunda, así no será fácil llegar a ellos, ya que el atacante deberá pasar primero por las capas superiores. A continuación, se explica cada una de las capas mencionadas:

- **Datos:** proteger los datos es lo más importante y es por ello que esta capa es la más interna del principio de defensa en profundidad. En un supuesto caso que el atacante hubiera logrado vulnerar las capas anteriores, los datos, que estarían contenidos en esta capa deberían estar cifrados, ya que es mucho más seguro que tener los datos en texto plano.
- **Aplicación:** hay una gran diversidad de aplicaciones, y son justamente éstas las que contienen los datos que se tienen que proteger, esto puede hacerse mediante el uso de controles de acceso, usando métodos de autenticación y autorización para acceder a las aplicaciones, también se pueden realizar evaluaciones de seguridad.

- **Equipo:** es importante que los equipos también se protejan, porque es en estos donde las aplicaciones se encuentran almacenadas y en muchos casos también los datos. En esta capa la protección hace referencia a los equipos de los usuarios y a los servidores, para protegerlos se pueden eliminar los servicios que no sean necesarios, dejando únicamente los de utilidad, también puede hacerse uso de un antimalware, el uso de contraseñas, parches de seguridad y escaneos de vulnerabilidades.
- **Red:** los equipos se conectan a través de las redes, por lo que su protección también es importante. Es recomendable subdividir la red de la organización dependiendo de su uso, para que en caso de que algún atacante acceda a la red se vea vulnerada solo una parte y no la red en su totalidad, porque el atacante al tener acceso a toda la red podría ver todo el tráfico que pasa por ella. La protección que se puede encontrar en esta capa es la creación de VLAN (Virtual Local Area Network, en español conocida como Red Virtual de Área Local), el uso de ACL (Access Control List o Listas de Control de Acceso), auditorías de seguridad, sistemas de detección de intrusiones, sistemas de prevención de instrucciones, uso de protocolos como SSL (Secure Socket Layer o Capa de Sockets Seguros), TLS (Transport Layer Security o Seguridad de la capa de transporte) o SSH (Secure SHell o Interprete de Órdenes seguro).
- **Perímetro lógico:** con esta capa se pretende asegurar el perímetro de la red, este puede verse como una “frontera” entre la red interna de la organización y las redes externas, tales como el internet o redes gestionadas por terceras personas. Es importante tener cuidado ya que el atacante podría tener acceso a las redes externas y aprovechar cualquier hueco de seguridad para intentar dañar la red de la organización. La seguridad de esta capa se concentra en los firewalls, pruebas de penetración, VPN (Virtual Private Network o Red Privada Virtual), entre otros.
- **Perímetro físico:** esta capa se refiere a la protección física de los equipos, es decir, debe evitarse que el atacante tenga acceso físico a la infraestructura, se puede hacer uso de diferentes herramientas, como la instalación de cámaras de video vigilancia, alarmas, bloqueo de cuartos de equipos, asimismo llevar un control de las actividades que realizan los usuarios en el sistema.
- **Políticas y procedimientos:** esta capa hace referencia a las reglas, obligaciones y procedimientos definidos por la organización para proteger y administrar su información, los integrantes de dicha organización deben de tener acceso a estas políticas para conocerlas, aplicarlas y seguirlas de manera adecuada.

  Aunado a esto, se debe de hacer un análisis de los recursos que se tienen y que se deben de proteger, asimismo se debe de realizar un análisis de las posibles amenazas que se puedan presentar para tener una respuesta rápida e intentar prevenir que la amenaza avance a la siguiente capa.

(Becolve Digital, 2019; Dávila, 2009; Guijarro Rodríguez et al., 2018; Leal, 2012; Moreno López, s. f.)

1.2 Normatividad de la seguridad informática

1.2.1. Normas de seguridad a través de la historia

Las normas son reglas que sirven como guía para un comportamiento determinado, estas proporcionan un marco de referencia, y su objetivo es evitar o minimizar los riesgos que se puedan producir.

Hay una gran variedad de normas que regulan el comportamiento en las diferentes sociedades, todas las personas tienen un vínculo a algún tipo de norma, como pueden ser normas jurídicas, morales, religiosas o técnicas, entre muchas otras que se pueden encontrar. En el ámbito de la seguridad informática hay normas de seguridad, las cuales ayudan a regir el comportamiento de los usuarios, equipos y sistemas computacionales, con el objetivo de proteger los activos.

A lo largo de los años, ha habido una gran cantidad de normas de seguridad las cuales han ayudado a las organizaciones a proteger su información, estas han evolucionado hasta llegar a las normas de la serie 27000, siendo estas las más conocidas.

Todo sistema informático por sí solo no tiene garantizada la seguridad, lo que se hace al aplicar dichas normas de seguridad es tratar de reducir los riesgos que se puedan presentar, además, la seguridad informática siempre se liga a dos elementos que son muy importantes, estos son el software y el hardware.

El propósito de los estándares es ser un punto de referencia y modelo a seguir para diseñar, desarrollar, implementar y medir la seguridad de los sistemas y productos, tomándose como referencia los criterios que use la organización, y los estándares internacionales permiten establecer un marco de referencia para las evaluaciones de seguridad de productos tecnológicos, estas evaluaciones se hacen siguiendo una metodología, mediante la cual se determina si el producto puede o no ser certificado y de acuerdo con los resultados obtenidos se puede determinar el nivel de confianza, e incluso los incidentes que puedan ocurrir y que pongan en riesgo la integridad, confidencialidad, autenticidad y disponibilidad del sistema.

Entre las organizaciones responsables de elaborar estándares a nivel internacional se encuentran la ISO y la IEC (International Electrotechnical Comission o Comisión Electrotécnica Internacional), estas organizaciones trabajan en conjunto para elaborar normas para las Tecnologías de la Información y la Comunicación.

(BSI Group, s. f.; Del Prado, 2013)

1.2.1.1 IEC – International Electrotechnical Comission

La International Electrotechnical Comission también conocida como IEC o en español Comisión Electrotécnica Internacional es la organización mundial no gubernamental que elabora estándares internacionales para las tecnologías eléctricas y electrónicas, que en su conjunto se conocen como electrotecnia.

Las normas IEC son un elemento importante para el comercio internacional, ya que al ser adoptadas por diversos países se reducen las barreras técnicas que producen o importan los productos y servicios. Asimismo, estas normas sirven como referencia al momento de crear contratos internacionales.

Las normas que elabora esta organización están basadas en el consenso, por lo que están representadas las necesidades principales de las naciones participantes, porque se toma en cuenta la participación de todos los miembros, sin importar su tamaño.

Estas normas son usadas por diseñadores, fabricantes, entidades de regulación, entidades públicas, etcétera, con la finalidad de que los productos operen de forma segura y eficiente en cualquier parte del mundo, reduciendo así las barreras de comercialización para proteger y proporcionar tranquilidad a los usuarios.

Esta organización fue creada en el año 1906, y su sede está en Ginebra, Suiza y actualmente está conformada por más de 170 países, más de 10,000 normas internacionales, más de 1 millón de certificados de conformidad y más de 20,000 expertos (IEC, s. f.; Odón de Buen, 2017)

1.2.1.2 ISO – International Organization for Standardization

La ISO que deriva del inglés International Organization for Standardization, conocida en español como Organización Internacional de Normalización, es una entidad no gubernamental que reúne expertos de todo el mundo, uno por país, incluyendo a los países desarrollados y países en vías de desarrollo, para compartir información y desarrollar estándares que faciliten el comercio, sirviendo tanto a los reguladores como a los consumidores. Se busca que las normas desarrolladas por esta organización sean adoptadas de manera voluntaria, siendo muy respetadas internacionalmente por el sector público y privado.

La ISO fue creada por la unión de dos organismos cuya función principal era la elaboración de estándares. Una de estas organizaciones fue la ISA que significa International Federation of the National Standardizing Associations o en español Federación Internacional de Asociaciones de Estandarización Nacionales, fue creada en 1926, aunque su fundación en Nueva York se remonta al año 1928. Esta organización desarrollaba sus actividades en Europa y su objetivo era considerar las áreas que no estaban reguladas por la IEC.

Cuando inició la Segunda Guerra mundial, la ISA intentó continuar con sus actividades, sin embargo, éstas fueron suspendidas cuando la comunicación internacional dejó de existir.

Tiempo después, a finales de 1944, en Londres nace el UNSCC o United Nations Standards Coordinating Committee conocida en español como Comité Coordinador de Estándares de las Naciones Unidas, cuya gestión se realizó desde las oficinas de la IEC, donde ya tenían una buena reputación gracias a Charles Le Maistre, quien es considerado el padre de la normalización, además él fue quien propició la fundación de la ISO.

En el año de 1945, hubo una reunión entre la UNSCC y la ISA, en dicha reunión se acordó construir una organización provisional, a la cual llamaron International Standards Coordinating Association. En 1946, en París se hizo una nueva reunión entre la ISA y el UNSCC, en donde la ISA se disolvería, esto por su inactividad durante la Segunda Guerra Mundial, al mismo tiempo, Le Maistre convocó a los delegados del UNSCC para que hicieran un cese de sus actividades debido al surgimiento de la nueva organización, la ISO, y es así como el 26 de octubre de 1946 se concluyó la reunión, con la International Organization for Standardization como el único organismo internacional de estandarización. Se puede decir, que la ISA fue la base para la creación de la ISO.

Finalmente, el 27 de febrero del año 1947 en Ginebra, Suiza es como inician las actividades de la ISO. En la actualidad, la ISO es la organización principal creadora de normas, elaborando hasta la fecha más de 20,000 normas las cuales abarcan muchos de los ámbitos de la fabricación de tecnología.

Las normas desarrolladas por la ISO y la IEC ofrecen el mismo nivel de protección, sin importar el tipo de economía que se trate, también se ocupan para la difusión de nuevas tecnologías y prácticas innovadoras, del mismo modo sirven de herramienta para la evaluación de conformidad y son usadas como mejora de confianza de productos, sistemas y servicios.

Estas normas también pueden convertirse en normas nacionales, pero para que esto pase deben pasar por un proceso que se lleva a cabo por algún organismo de normalización del país, y también pueden convertirse en reglamentos técnicos nacionales, sin provocar barreras técnicas.

En los siguientes apartados se profundiza en la historia de los estándares desarrollados por las diferentes organizaciones, estándares estadounidenses, europeos, e internacionales, que han tenido un papel importante dentro de la seguridad informática.

También hay que destacar que se cuenta con organizaciones a nivel europeo que emiten normas, entre ellas se encuentra el Comité Europeo de Normalización también conocido como CEN, el Instituto Europeo de Normalización Electrotécnica o CENELEC y el Instituto Europeo de Normas de Telecomunicaciones, en inglés European Telecommunications Standards Institute o ETSI.

(Carvajal Herrera, 2013; Grupo ESGinnova, 2015; Iriarte Medina, 2006)

1.2.2 Criterios comunes / ISO 15408

Los Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información o CC derivado del inglés Common Criteria o Criterios Comunes fueron desarrollados por los gobiernos de Canadá, Francia, Alemania, los Países Bajos, el Reino Unido y Estados Unidos a mediados de la década de los 90. Los Criterios Comunes buscaron unificar estándares existentes, como el ITSEC, el TCSEC y el CTCPEC, con el objetivo de evitar una reevaluación de productos dirigidos al mercado internacional.

En Estados Unidos, en la década de 1980 se desarrollaron criterios de seguridad, que llevaban por nombre Trusted Computer System Evaluation Criteria o TCSEC, este conjunto de criterios es mejor conocido como *"El libro naranja"* debido al color de su portada. Este libro tomó una gran importancia, ya que sirvió como base para que otros países desarrollaran especificaciones flexibles, que se adaptaran a la evolución de los sistemas de TI.

Tomando como base el TCSEC, en 1991, la comisión europea publica el ITSEC, y en el año 1993 en Canadá, surgen los criterios CTCPEC, los cuales son la unión de los criterios americanos y europeos, en ese mismo año, el gobierno de Estados Unidos dió a conocer los Criterios Federales o Federal Criteria, los cuales son la unificación de los criterios europeos y americanos.

Con el objetivo de normalizar estos criterios es como la ISO a principios de la década de los 90 brinda la certificación ISO-IEC 15408, esta certificación es el resultado de la negociación entre diferentes países de Europa, América, África y el continente australiano.

A continuación, se hablará de los estándares antes mencionados.

1.2.2.1 Trusted Computer System Evaluation Criteria (TCSEC) – Libro Naranja

El Trusted Computer System Evaluation Criteria,por sus siglas en inglés TCSEC, también conocido como *Libro Naranja* o Criterios de Evaluación del Sistema Informático de Confianza fue propuesto en el año 1983, tenía como objetivo proveer políticas de seguridad de hardware, firmware y software, dichas políticas se encargan de preservar la confidencialidad de la información clasificada. Según el Departamento de Defensa también conocido como DOD o Department of Defense, hay varios niveles de seguridad, los cuales indican qué tan bien se encuentra protegido el software, el hardware y la información almacenada.

Es así como surge el 15 de agosto de 1983 el primer libro de esta serie, cuyo color de portada es naranja, de ahí que sea conocido como *"el libro naranja".* Este libro fue elaborado por el National Computer Security Center por sus siglas en inglés NCSC que en español significa Centro Nacional de Ciberseguridad de la NSA (National Security Agency o Agencia de Seguridad Nacional) del DOD.

Los TCSEC definen un conjunto de criterios compuesto de cuatro divisiones: A, B, C y D, las cuales se explican a continuación.

División D: Protección mínima.

Esta división está corresponde a los sistemas que no es necesario que sean evaluados, esto debido a que no cuentan con protección para el hardware y tampoco con algún tipo de autenticación por lo que el sistema puede verse comprometido fácilmente.

División C: Protección discrecional

Este nivel se encuentra dividido en las clases C1 y C2.

- **C1. Protección de seguridad discrecional:** este tipo de sistemas ofrece características de seguridad limitadas, es decir, los usuarios con el mismo nivel pueden compartir procesamiento sin dañar el sistema.

  Este tipo de sistemas tiene dos características principales, la primera de ellas es contar con un mecanismo de autenticación para acceder al sistema, la otra es la protección de archivos, para así decidir quien tiene los permisos necesarios para acceder a uno u otro archivo almacenado.

  Teniendo este nivel de seguridad el sistema no queda exento de verse comprometido, sin embargo, ya no sería tan fácil, con la autenticación se habilitarían y deshabilitaría el contenido correspondiente a cada usuario, y solamente el administrador del sistema es quien puede realizar modificaciones, este usuario es conocido como root.

- **C2. Protección de acceso controlado:** estos sistemas proporcionan un mayor nivel de seguridad que C1. El sistema proporciona control individual por medio de una autenticación, donde todas las acciones que realice quedan registradas por lo que, si algún usuario provoca un incidente, el sistema sería capaz de saber quién lo provocó.

  Estos sistemas también son capaces de permitir que los usuarios accedan por medio de listas de control de acceso, por lo que a los usuarios se le podría permitir o denegar alguna acción sobre los archivos u objetos almacenados.

  Esta clase tiene como característica fundamental la auditoría, la cual es usada para tener registro de los eventos asociados con la seguridad, incluida la actividad del administrador del sistema por lo que la auditoría debe tener una autenticación adicional.

División B. Protección mandatoria.

Este nivel se seguridad cuenta con tres clases, B1, B2 y B3.

- **B1. Seguridad etiquetada:** tiene controles de acceso que son obligatorios, para que solo los usuarios con cierta clasificación puedan o no tener acceso a los diferentes archivos, esto es lo que se conoce como seguridad etiquetada. Este es el primer nivel que admite clasificaciones de seguridad de múltiples niveles.
- **B2. Protección estructurada:** en esta clase se mejoran las características de la clase B1, por lo que el libro naranja dice que los sistemas B2 son "resistentes a la penetración". Estos sistemas necesitan mayor modularidad, asimismo se requiere el uso de características de hardware con el objetivo de aislar funciones de seguridad, también es necesario que haya un administrador, el cual se encargará de gestionar la configuración del sistema, los cambios en el código y la documentación.
- **B3. Dominios de seguridad:** en esta clase, las funciones de seguridad y el diseño del sistema son más estrictos. También, es necesario contar con procedimientos que se aseguren de que la seguridad no falle, asimismo se requiere una administración confiable de recursos, entre otros. Este nivel de seguridad necesita que las terminales de los usuarios se conecten al sistema mediante accesos seguros. Cabe mencionar que este tipo de sistemas no son muy comunes.

División A. Protección verificada.

Este es el nivel de seguridad más alto del libro naranja, para lograr esto se deben incluir los componentes de los niveles anteriores, el diseño debe de ser verificado, además se debe hacer un análisis de los canales ocultos y la distribución tiene que ser confiable, es decir, que el hardware y el software se hayan protegido durante su entrega para evitar incidentes de seguridad.

(Chamorro López, 2011; Cortes Monroy, 2002; Iriarte Medina, 2006; Pearson, 2013)

1.2.2.2 Information Technology Security Evaluation Criteria (ITSEC) – Libro Blanco

El ITSEC o Information Technology Security Evaluation Criteria o también conocido como el *libro blanco* o Criterios de Evaluación de Seguridad en Tecnologías de la Información es un conjunto de criterios que ayudan a evaluar la seguridad de los sistemas, estos fueron desarrollados por Francia, Alemania, Los Países Bajos y el Reino Unido.

Para desarrollarlo, estos países tomaron como base el libro naranja, y tenía como objetivo proporcionar confianza al usuario, para que sintiera la seguridad de que el sistema que está adquiriendo cuenta con los requisitos de seguridad especificados, definiendo a la seguridad como el conjunto de disponibilidad, integridad y confidencialidad.

El ITSEC se refiere a los productos y sistemas como TOE cuyas siglas significan Target Of Evaluation o en español Objetivo de Evaluación, estos se componen de elementos de hardware

y software, teniendo la diferencia principal en su entorno, ya que para un producto el entorno es algo muy general, mientras que para un sistema el entorno debe ser algo muy específico. Un TOE es un producto o sistema de TI, el cual está sujeto a una evaluación de seguridad.

De acuerdo con el ITSEC, el proveedor es quien presenta el objetivo de seguridad que debe ser evaluado, además, define los mecanismos necesarios para determinar las funciones de seguridad, del mismo modo, especifica cuales serán las funciones de seguridad del TOE y las posibles amenazas. Se debe tener la seguridad de que dichas funciones cumplen con los objetivos de seguridad establecidos, y esto a su vez tiene relación con que las funciones implementadas sean correctas y efectivas.

Los participantes del proceso de evaluación de productos son:

1. Sponsor o proveedor
2. CLEF (Commercial Licensed Evaluation Facilities o Instalaciones de Evaluación con Licencia Comercial)
3. Cuerpo de certificación.

Este proceso de evaluación consta de 5 fases, las cuales se describen a continuación.

Paso 1. La decisión de evaluar

Esta decisión se basa en un análisis de costo – beneficio en un negocio. Hay que establecer patrones de demanda para los productos o proyectos relacionados a oportunidades específicas, dependiendo del negocio que se trate, incrementando así su potencial.

Paso 2. Preparación para la evaluación

En este paso se especifican las características de seguridad del producto, así mismo se especifican los objetivos de seguridad, las amenazas y el ambiente dentro del cual el producto puede operar, también es necesario especificar el nivel se seguridad, este nivel de seguridad va del nivel E0 al E6, y también se especifican las funciones de seguridad.

Niveles de seguridad

- **E0:** este nivel no emite un certificado, ya que representa un aseguramiento inadecuado.
- **E1:** en este nivel debe haber una meta de seguridad, así como una descripción no formal del diseño del TOE.
- **E2:** se debe de añadir lo requerido del nivel E1, además se debe de incluir una descripción informal del diseño detallado, y se tienen que evaluar pruebas de ensayos funcionales, inclusive para la configuración tiene que haber un sistema de control, además de un procedimiento adecuado de distribución.
- **E3:** además de incluir lo anterior, se debe de evaluar el código fuente, esquemas de hardware y también se deben de evaluar las pruebas de los ensayos realizados.

- **E4:** debe añadirse un modelo normal subyacente de políticas de seguridad, además, debe ser especificado el diseño detallado.
- **E5:** a este nivel de seguridad debe añadirse una correspondencia entre el diseño detallado, el código fuente y los esquemas de hardware.
- **E6:** al ser el último nivel, deben de especificarse formalmente cuáles serán las funciones dedicadas a la seguridad, asimismo, el diseño arquitectónico debe de ser coherente con el modelo formal y las políticas de seguridad especificadas.

(Iriarte Medina, 2006)

Funciones de seguridad

- **F-C1:** proporciona un control de acceso discrecional.
- **F-C2:** proporciona un control de acceso discrecional, identificando a los usuarios por medio de procesos de identificación y aislamiento de recursos.
- **F-B1:** se incluyen funciones de control de acceso para los usuarios y objetos de almacenamiento que están bajo su control.
- **F-B2:** esta función refuerza los requisitos de autentificación de la clase anterior.
- **F-B3:** proporciona funciones de soporte a los roles de administración de seguridad, y se amplía la auditoría para señalar sucesos relevantes para la seguridad.
- **F-IN:** esta función es para los sistemas con requisitos de alta integración para datos y programas, como lo son las bases de datos.
- **F-AV:** esta función establece requisitos elevados para la disponibilidad de un sistema completo o de funciones especiales del sistema, con estos requisitos se controlan los procesos de fabricación.
- **F-DI:** se establecen requisitos relativos a la protección de la integridad de los datos durante su intercambio.
- **F-DC:** está dirigida a los sistemas con altas demandas de confidencialidad de los datos durante su intercambio.
- **F-DX:** está dirigida a redes con alta demanda de confidencialidad e integridad de la información que se intercambia.

(Iriarte Medina, 2006)

Paso 3. Evaluación.

Este es un proceso de prueba, el cual verifica que se hayan cumplido los requerimientos. En esta etapa los evaluadores se encargan de evaluar el objetivo de seguridad, la exactitud del sistema y el ambiente de operación, además, se generan los reportes de evaluación.

Paso 4. Certificación.

Si después de la evaluación los expertos determinan que se ha alcanzado la seguridad que se busca, se proporciona la certificación, si esto no es así y no se alcanza el nivel de seguridad

deseado, el proveedor y el certificador se ponen de acuerdo con las modificaciones necesarias que se tengan que hacer.

Paso 5. Re-Evaluación.

Si un producto tiene que ser modificado la reevaluación es necesaria. Se puede hacer una clasificación del producto de acuerdo con las características de seguridad, esta clasificación puede usarse para determinar qué impacto tendría el producto en la certificación y las medidas que deben tomarse. Que el producto o servicio obtenga la certificación es importante, ya que con esto el usuario se sentiría más seguro, porque sabría el nivel de seguridad de lo que está adquiriendo.

Después de que fue publicado el ITSEC, los países autores comenzaron con la elaboración de un boceto de una metodología que acompañara a estos criterios, y es así como en 1993 con el apoyo de SOGIS (Senior Officials Group Information Systems Security o Grupo de Altos Funcionarios de Seguridad de los Sistemas de Información) surge la versión 1.0 de ITSEM, cuyo objetivo específico es asegurar que hay métodos de evaluación que complementan al ITSEC, dicha evaluación se refiere a la seguridad de los productos y sistemas de TI, no incluye medidas físicas, organizativas, administrativas o de personal, que no estén relacionadas con TI. ITSEC e ITSEM están dirigidos a los evaluadores, patrocinadores, certificadores, suministradores, desarrolladores, acreditadores de sistemas y usuarios.

(CCN CERT, s. f.-b; Cortes Monroy, 2002; Iriarte Medina, 2006; Pearson, 2013)

1.2.2.3 Canadian Trusted Computer Product Evaluation Criteria – CTCPEC

El Canadian Trusted Computer Product Evaluation Criteria o Criterios de Evaluación de Productos Informáticos de Confianza de Canadá, también conocido como CTCPEC, es un estándar de seguridad informática el cual se publicó en 1993, por el Communicatios Security Establishment Canada, su objetivo es proporcionar un criterio de evaluación de productos de TI y surge de combinar los criterios TCSEC y el ITSEC, cabe mencionar que el CTCPEC condujo a la creación del estándar Common Criteria que se revisa más adelante.

Puede decirse que estos criterios son la versión canadiense del *libro naranja,* e incluso pueden verse como una versión más flexible.

Dentro de estos criterios se encuentran cuatro criterios funcionales y dieciocho servicios de seguridad, los cuales se acomodan de la siguiente manera:

- Confidencialidad
    - Canales encubiertos
    - Confidencialidad discrecional

    - Confidencialidad obligatoria
    - Reutilización de objetos

- Integridad
    - Integridad de dominio
    - Integridad discrecional
    - Integridad física
    - Restauración
    - Separación de bienes.

- Disponibilidad
    - Contención
    - Tolerancia a fallos
    - Robustez
    - Recuperación.

- Responsabilidad
    - Auditoría
    - Identificación y autentificación
    - Vía confiable.

El CTCPEC se puede aplicar a una gran variedad de productos, entre los cuales están los sistemas de multiproceso, sistemas distribuidos y redes, además de incluir funcionalidades que garantizan la seguridad multilateral.

(Chamorro López, 2011; Dávila, 2009; DBpedia, s. f.; Pearson, 2013)

1.2.2.4 ISO 15408 – Common Criteria (CC)

Los Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información o mejor conocidos como Criterios Comunes o Common Criteria, abreviados como CC, fueron desarrollados a mediados de la década de los 90 por los gobiernos de Canadá, Francia, Alemania, Países Bajos, Reino Unido y Estados Unidos, con la finalidad de unificar los estándares de evaluación de seguridad de productos que existían hasta ese momento, con el objetivo de que hubiera un solo proceso de evaluación en diferentes países.

Los estándares que se unifican en los Criterios Comunes son el TCSEC, ITSEC y CTCPEC, al hacer esto se evitaba la reevaluación de productos que estaban dirigidos al mercado internacional.

La versión 1.0 de los CC fue publicada en 1996, la versión 2.0 se publicó en el año 1998, y en el año de 1999 se convirtió en el estándar ISO/IEC 15408. En mayo del año 2000 se firmó un acuerdo que permite el reconocimiento mutuo de los certificados de CC. Los participantes de este acuerdo tienen en común los siguientes objetivos:

1. Garantizar que las evaluaciones realizadas a los productos y perfiles de protección se hagan con estándares altos.
2. Eliminar la reevaluación de productos de TI y de los perfiles de protección.
3. Hacer mas eficiente el proceso de evaluación y certificación de los perfiles de protección y productos de TI.

En la actualidad, los CC representan uno de los principales organismos que permiten identificar de manera objetiva las necesidades de seguridad de los usuarios, estos criterios también permiten identificar a los productos que cumplen con dichas características.

La norma ISO/IEC 15408 se compone de tres partes, las cuales se describen a continuación:

Parte 1. Introducción y modelo general

Es la introducción a los CC, se definen los conceptos y principios generales de la evaluación de seguridad de TI y muestra un modelo general de evaluación, adicionalmente, determina como es que pueden realizarse las especificaciones de los sistemas y/o productos, poniendo atención a la seguridad de la información y su tratamiento.

Los CC están destinados a ser usados como base para evaluar las propiedades de seguridad de productos y sistemas de TI, además, permiten hacer una comparación de los resultados de las evaluaciones de seguridad independientes, asimismo, proporcionan un conjunto de requisitos funcionales de seguridad, cuyo objetivo es garantizar la implementación de medidas de seguridad a lo largo de la evaluación, con los resultados obtenidos los consumidores sabrán si el producto y/o sistema evaluado es seguro.

La seguridad de los CC está dirigida a preservar la integridad, disponibilidad y confidencialidad de la información, incluso pueden aplicarse a las medidas de seguridad implementadas en el hardware, el software y el firmware.

Hay tres grupos de interés general en la evaluación de seguridad de productos y sistemas de TI, los cuales se enlistan a continuación:

- **Consumidores:** los CC permiten saber si la evaluación realizada cubre las necesidades de los diferentes consumidores, ya que pueden usar los resultados de la evaluación para saber si el producto y/o sistema cumple con sus necesidades de seguridad, también pueden usar los resultados para comparar diferentes productos y/o sistemas.
- **Desarrolladores:** usan los CC para preparar la evaluación de sus productos e identificar los requisitos de seguridad que debe de cumplir el TOE, también pueden usarse para ver que pruebas son necesarias para la evaluación.

- **Evaluadores:** los CC contienen los criterios usados por los evaluadores para revisar que tanto cumple el TOE con los criterios establecidos, hay que notar que los CC no especifican un procedimiento guía para cumplir con los criterios.

El TOE es un producto o sistema de TI, es decir, es el objeto que se va a evaluar, el cual se define acorde a lo siguiente:

- **TSP – TOE Security Policy o Políticas de Seguridad del TOE:** definen las reglas mediante las cuales se accede, gestiona, protege y se distribuyen los recursos, información y servicios controlados por el TOE.
- **SFP's – Security Function Policies o Función de las Políticas de Seguridad:** son las que se definen en el TSF, cada uno de los SFP tiene un alcance de control que define los asuntos, objetos y operaciones.
- **SF – Security Function o Función de Seguridad:** implementa la SFP, son mecanismos que proporcionan características necesarias de seguridad.
- **TSF – TOE Security Functions o Funciones de Seguridad del TOE:** es todo el hardware, software y firmware que está directa o indirectamente relacionado con las TSP.
- **TSFI – TOE Security Functions Interfaces o Interfaces de las Funciones de Seguridad del TOE:** son las interfaces mediante las cuales interactúan los usuarios o aplicaciones con los recursos o información.

(Chamorro López, 2011)

Los CC pueden ser usados como referencia en las áreas interesadas por la seguridad de las TI, por ejemplo, los oficiales de seguridad de los sistemas, los auditores tanto internos como externos, las entidades evaluadoras de seguridad, entre otros.

Parte 2. Requisitos funcionales de seguridad

Se establece un conjunto de componentes funcionales, los cuales son usados para especificar los requisitos de funcionalidad de los TOE, este tipo de requerimientos son los que definen el comportamiento de seguridad que debería tener el TOE, y están organizados en once clases, las cuales se denominan *clases de requerimientos funcionales,* cada una de estas clases se encarga de cubrir las necesidades de un área en específico. Las clases mencionadas se explican a continuación:

- **FAU – Auditoría de seguridad:** las auditorías de seguridad están relacionadas con las actividades de seguridad, se ve involucrado un análisis de información. Con el resultado de las auditorías se puede determinar cuales fueron las actividades relevantes, así como al usuario responsable.
- **FCO – Comunicaciones:** esta clase permite garantizar la identidad del creador y del receptor de la información, además, se asegura de que el creador no pueda negar que

fue quien envió el mensaje y que el receptor no niegue que fue quien recibió la información.

- **FCS – Soporte criptográfico:** las funciones de seguridad del TOE pueden llevar consigo operaciones criptográficas como camino y canal confiable, autenticación, identificación, entre otras, con el objetivo de cubrir los requisitos de seguridad de alto nivel. La clase FCS es usada cuando en el TOE hay funciones de cifrado en hardware, software y firmware.
- **FDP – Protección de datos de usuario:** esta clase incluye requisitos para funciones de seguridad del TOE, contiene políticas de seguridad que se relacionan con la protección de los datos de los usuarios.
- **FIA – Identificación y autenticación de usuario:** esta clase se relaciona con las funciones que comprueban la identidad de los usuarios, usa la autenticación e identificación, mismas que permitirán comprobar los atributos de seguridad de cada usuario, ya que para poner en prácticas las políticas de seguridad es necesario identificar los permisos con los que cuenta cada uno.
- **FMT – Gestión de la seguridad:** se especifica la administración de las funciones de seguridad del TOE, sus objetivos son: administrar los atributos y funciones de seguridad, así como los datos de las funciones de seguridad, y también se encarga de definir los perfiles de seguridad.
- **FPR – Privacidad:** clase que engloba los elementos de privacidad que proporcionaran protección a los usuarios, es decir, evitará que otros usuarios hagan mal uso de su información
- **FPT – Protección de las funciones de seguridad del objeto a evaluar:** está relacionada con los mecanismos que brindan seguridad al TOE, además se encarga de proteger los datos de sus funciones de seguridad para que estos no sean alterados.
- **FRU – Utilización de recursos:** esta clase se relaciona con la disponibilidad de los recursos.
- **FTA – Acceso al objeto de evaluación:** en esta clase se especifican los requisitos funcionales que sirven para gestionar la creación de sesiones de usuario.
- **FTP – Caminos/canales confiables:** un canal confiable hace referencia a un canal de comunicación iniciado por cualquiera de sus extremos, siendo su característica principal el no repudio, mientras que un camino confiable es aquel que brinda un medio por el cual los usuarios pueden autenticarse.

  En esta clase se brindan los requisitos que se necesitan para la creación de caminos confiables entre las funciones de seguridad y los usuarios, y entre las funciones de seguridad y otros productos de TI. Las características de los caminos y canales confiables son:
    - Para construir los caminos de comunicación se usan canales que pueden ser internos o externos, estos se aíslan para los datos de las funciones de seguridad de los comandos de las mismas funciones, así como de los datos de usuario.

- Los caminos de comunicación pueden ser iniciados por el usuario o por el TSF.
- Los caminos de comunicación pueden garantizar que el usuario se está comunicando con la TSF correcta y que la TSF se está comunicando con el usuario correcto.

Parte 3. Requisitos de garantía de seguridad.

Esta tercera parte se destina a los desarrolladores de TI, esto porque se definen los criterios de confiabilidad que deben de usar los evaluadores para comprobar el desempeño de los desarrolladores y de los productos. Estos requisitos de garantía se componen de dos partes, la primera de ellas son las clases de garantía y la segunda son los niveles de garantía, los cuales se explicarán a continuación.

Clases de garantía

Las clases de garantía son los requerimientos que se necesitan para mantener la seguridad que proporciona el TOE, se encuentran divididos en siete clases, las cuales se explican a continuación.

- **ACM – Gestión de la configuración:** esta clase sirve para mantener la integridad del TOE, esto se puede lograr teniendo un control sobre los procesos de modificación y refinamiento del TOE. La administración de la configuración evitará que se hagan modificaciones no autorizadas, esto garantiza que tanto el TOE como la documentación que se usó en la evaluación sean los mismos que se usarán en la distribución.
- **ADO – Operación y entrega:** define los requisitos de los procedimientos y normas relacionadas con el uso operacional seguro del TOE, también asegura que la protección que ofrece el TOE no se compromete antes, durante y después de su funcionamiento.
- **ADV – Desarrollo:** en esta clase se definen los requerimientos para el desarrollo del TSF paso a paso, comenzando con la especificación, además resume el proceso iniciando con la declaración de seguridad hasta llegar a la implementación final del TOE. Cada TSF resultante brinda información al evaluador, quien con esta información verifica si se han cumplido los requerimientos funcionales del TOE.
- **AGD – Documentación y guías:** aquí se definen los requisitos dirigidos a la comprensión, cobertura e integridad de la documentación para usuarios y administradores que proporciona el fabricante.
- **ALC – Ciclo de vida:** se definen los requerimientos de garantía mediante la adopción de un ciclo de vida previamente definido el cual incluya los pasos involucrados en el desarrollo del TOE, asimismo, se incluyen cosas adicionales como las políticas para solucionar los fallos, el uso correcto que debería darse a las herramientas, así como las medidas de seguridad que protegerán al entorno de desarrollo.
- **ATE – Prueba:** se establecen los requisitos que deberán tener las pruebas para que se demuestre que el TSF cumple con los requerimientos de seguridad funcionales del TOE.

- **AVA – Evaluación de vulnerabilidades:** se definen requisitos que servirán para identificar vulnerabilidades en el TOE.

Aunado a lo anterior, los CC incluyen una clase específica para los requerimientos del mantenimiento de la garantía, la cual es la siguiente:

- **AMA – Mantenimiento de garantías:** esta clase pretende mantener el nivel de garantía del TOE, con la finalidad de que siga cumpliendo su declaración de seguridad a medida que se vayan haciendo cambios en el TOE o en su entorno. Se identifican las acciones que el fabricante y el evaluador deben realizar después de que el TOE haya sido evaluado exitosamente.

Como complemento a la evaluación, también se incluyen dos clases más, una clase de requisitos específicos para evaluar los Perfiles de Protección, cuya abreviación es PP y la otra para la evaluación de los objetivos de seguridad, también conocidos como ST, que se explican a continuación:

- **APE – Evaluación de perfiles de protección:** es un conjunto de requisitos funcionales y de garantías independientes que identifican a un conjunto de objetivos de seguridad, estos especifican lo que se necesita respecto a la seguridad en un dominio determinado.
- **ASE – Evaluación de objetos de seguridad:** es un conjunto de requisitos funcionales y de garantías que se usan como especificaciones de seguridad de un producto o sistema en concreto, especifican los requisitos de seguridad que proporciona o los que satisface el producto o sistema, basados en su implementación.

Niveles de garantía de evaluación

Los CC fueron creados de una manera flexible, lo que permite que se integren los diferentes sistemas que existen para la evaluación, certificación y acreditación de seguridad de las TI. También se pueden especificar las funcionalidades de los productos en términos de PP y seleccionar alguno de los siete niveles de garantía de evaluación o EAL, los cuales se explican a continuación:

- **EAL1 – funcionalidad probada:** se aplica cuando las amenazas no son vistas de una manera seria, este nivel se seguridad garantiza que las funciones del TOE son coherentes con su documentación y que proporciona protección contra para las amenazas que se identificaron.
- **EAL2 – estructuralmente probado:** proporciona confianza realizando un análisis de las funciones de seguridad y haciendo uso de los manuales y el diseño de alto nivel, con lo anterior se puede comprender el comportamiento de la seguridad, y mediante pruebas de caja negra se comprueba si el desarrollador realizó un análisis de vulnerabilidades.
- **EAL3 – probado y verificado metódicamente:** el análisis realizado en este nivel hace uso de pruebas de caja gris lo que permite al desarrollador alcanzar un mayor nivel de seguridad.

- **EAL4 – diseñado, probado y revisado metódicamente:** este nivel permite que el desarrollador alcance niveles de seguridad aun mayores, basándose en las buenas prácticas, mismas que no requieren de otros recursos ni de conocimiento especializado. El análisis que se realiza hace uso del diseño de bajo nivel de cada uno de los módulos del producto, además se buscan vulnerabilidades, las cuales son independientes de las pruebas que ya haya realizado el desarrollador.
- **EAL5 – diseñado y probado semiformalmente:** permitirá tener una máxima garantía de ingeniería de seguridad positiva, esto se logra aplicando procedimientos de seguridad de manera moderada. La confianza se respalda con un diseño del alto nivel, una presentación semiformal de los requisitos funcionales y de un modelo formal, además se debe demostrar que es capaz de resistir ataques de penetración
- **EAL6 – diseño verificado y probado semiformalmente:** el análisis realizado en este nivel hace uso de un diseño modular, asimismo, el escaneo de vulnerabilidades tiene que demostrar que el producto es sumamente resistente a los ataques de penetración. Se considera que el objeto que se está evaluando es de gran valor, también se considera que el tipo de análisis de este nivel se puede aplicar a objetos que tienen como objetivo mantener la seguridad en situaciones de riesgo alto.
- **EAL7 – diseño verificado y probado formalmente:** este nivel se aplica en el desarrollo de objetos de evaluación de seguridad para situaciones donde el riesgo es muy alto, donde la seguridad está fuertemente relacionada con la funcionalidad. En este nivel el evaluador confirma los resultados obtenidos de las pruebas de caja blanca que el desarrollador realizó.

Estos niveles de garantía de evaluación proporcionan un nivel de confianza esperado al TOE que se está analizando, éste puede incluir sistemas operativos y distribuidos, aplicaciones y redes de computadoras.

La filosofía de los CC afirma que a mayor esfuerzo en la evaluación se consigue una mayor garantía, este nivel creciente de esfuerzo se basa en:

- **El alcance:** cuando el producto o sistema de TI es más grande o se involucra en mayor parte, el esfuerzo en la evaluación es mayor.
- **La profundidad:** entre más finos sean el nivel de diseño y los detalles, el esfuerzo en la evaluación será mayor.
- **El rigor:** entre más estructurado se aplique, el esfuerzo en la evaluación será mayor.

La evaluación de un TOE se realiza con los criterios de evaluación mencionados en la tercera parte, dicha evaluación tiene como objetivo mostrar que el TOE cumple con los requerimientos de seguridad.

Con la evaluación se deben de obtener resultados objetivos los cuales pueden usarse como pruebas, por lo tanto, el resultado de esta evaluación permite saber que tanto se puede confiar en el TOE.

(CC Portal, 2013; CCN CERT, s. f.-a; Chamorro López, 2011; López Barrientos & Quezada Reyes, 2019; Pearson, 2013)

1.2.3. COBIT – Control Objetives for Information and Related Technologies

El Control Objectives for Information and Related Technologies, abreviado como COBIT y conocido en español como Objetivos de Control para la Información y Tecnologías Relacionadas, es un marco de referencia creado con la finalidad de ayudar a las organizaciones a desarrollar, organizar e implementar estrategias para la gobernanza, y mantener un equilibrio entre los beneficios, los recursos utilizados y los niveles de riesgo, puede aplicarse a diferentes organizaciones sin importar su tamaño o si pertenecen al sector público o al privado. COBIT fue desarrollado con la finalidad de ser aceptado para realizar buenas prácticas de seguridad y control en las TI.

En 1995 surgió el proyecto COBIT, su objetivo principal era tener un gran impacto en los negocios y en los sistemas de TI, este estándar tiene sus fundamentos en los objetivos de la Fundación de Auditoría y Control de Sistemas de Información, por sus siglas en inglés ISACF, que significan Information Systems Audit and Control Foundation, los cuales fueron mejorados con estándares internacionales específicos de la industria.

En 1996 se publicó la primera versión de este estándar, la segunda versión se publicó en 1998, donde se adicionaron las guías de gestión. En el 2000 se publicó la tercera versión, y en el año 2003 COBIT fue mejorado, introduciendo el aumento del control gerencial, el desarrollo de gobierno de TI y el manejo del desempeño. A finales del año 2005 se publicó la versión cuatro y en mayo del año 2007 surgió la versión 4.1.

Fue hasta el 2012 cuando se liberó la versión cinco, es en esta versión donde se unen varios marcos de referencia: COBIT 4.1, Val IT 2.0 y Risk IT, también se integra el Modelo de Negocios para la Seguridad de la Información conocido como BMIS que proviene del inglés Business Model for Information Security y el Marco de Referencia para el Aseguramiento de la Tecnología de la Información abreviado como ITAF, que proviene del inglés Marco de Referencia para el Aseguramiento de la Tecnología de la Información.

Desde finales del año 2018, COBIT 2019 está disponible, este nuevo marco de referencia es más completo y coherente, su diseño permite que haya actualizaciones de manera más frecuente. Su objetivo principal es construir estrategias de gobernanza que sean más flexibles y que puedan adaptarse y evolucionar con los avances tecnológicos, además de enfatizar la importancia de la información en las organizaciones.

Adicionalmente, este nuevo marco puede adaptarse a otras metodologías, como ITIL (Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologias de Información), CMMI (Capability Maturity Model Integration o Integración de Modelos de Madurez

de Capacidades) y TOGAF (The Open Group Architecture Framework o Esquema de Arquitectura del Open Group), por lo que puede ser muy útil para unificar los procesos de toda la organización.

En COBIT 5 se tenían cinco principios, y en la versión 2019 se tienen seis principios del sistema de gobierno y tres principios del marco de gobierno.

Los seis principios que se presentan a continuación son los requisitos principales que debe tener un sistema de gobierno para administrar la información y tecnología corporativa:

1. Las organizaciones necesitan un sistema de gobierno para cubrir las necesidades de los stakeholders (interesados), es decir, se tiene que proporcionar valor a los stakeholders, y se tiene que lograr un equilibrio entre los beneficios, los riesgos y los recursos.
2. Un sistema de gobierno tiene diferentes componentes, los cuales pueden trabajar juntos sin problema.
3. Los sistemas de gobierno tienen que ser dinámicos, esto quiere decir que si hay cambios en los factores de diseño por más mínimos que sean hay que tener en cuenta el impacto que tienen en el sistema EGIT.
4. Debe separarse el gobierno de la gestión.
5. El sistema de gobierno tiene que adecuarse para cubrir las necesidades de la organización priorizando sus componentes, usando como parámetro los factores de diseño.
6. El sistema de gobierno debe satisfacer las necesidades de toda la empresa, poniendo atención en toda la información que usa la empresa para cumplir sus objetivos.

Los puntos que se muestran a continuación definen los principios básicos de un marco de gobierno, los cuales permiten crear un sistema de gobierno:

1. Para permitir que la coherencia sea maximizada y la automatización sea permitida, el marco de gobierno tiene que tomar como base el modelo que distinga los componentes clave y la relación que tienen entre sí.
2. Los marcos de gobierno tienen que admitir que se añada nuevo contenido, asimismo, deben dar oportunidad de afrontar flexiblemente nuevos problemas.
3. Los marcos de gobierno tienen que ser capaces de adaptarse a regulaciones y estándares relevantes.

Objetivos de gobierno y objetivos de gestión

Los objetivos de gobierno y los objetivos de gestión están agrupados en cinco dominios, el primer dominio es EDM (Evaluar, Dirigir y Monitorear), este reúne los objetivos de gobierno, mientras que los objetivos de gestión se reúnen en los cuatro dominios restantes: APO (Alinear,

Planificar y Organizar), BAI (Construir, Adquirir e Implementar), DSS (Entregar, Dar servicio y Soporte) y MEA (Monitorear, Evaluar y Valorar).

Estos objetivos deben de alinearse con los objetivos de la empresa, en total son cuarenta objetivos, de los cuales cinco son de gobierno y treintaicinco de gestión.

Los objetivos de cada dominio se muestran a continuación:

EDM – Evaluar, Dirigir y Monitorear:

- **EDM01:** asegurar el establecimiento y el mantenimiento del marco de gobierno.
- **EDM02:** asegurar la entrega de beneficios.
- **EDM03:** asegurar la optimización del riesgo.
- **EDM04:** asegurar la optimización de recursos.
- **EDM05:** asegurar la participación de las partes interesadas.

APO – Alinear, Planificar y Organizar:

- **APO01:** gestionar el marco de gestión de información y tecnología.
- **APO02:** gestionar la estrategia.
- **APO03:** gestionar la arquitectura empresarial.
- **APO04:** gestionar la innovación.
- **APO05:** gestionar el portafolio.
- **APO06:** gestionar el presupuesto y los costes.
- **APO07:** gestionar los recursos humanos.
- **APO08:** gestionar las relaciones.
- **APO09:** gestionar los acuerdos de servicio.
- **APO10:** gestionar los proveedores.
- **APO11:** gestionar la calidad.
- **APO12:** gestionar los riesgos.
- **APO13:** gestionar la seguridad.
- **APO14:** gestionar los datos.

BAI – Construir, Adquirir e implementar:

- **BAI01:** gestionar los programas.
- **BAI02:** gestionar la definición de requerimientos.
- **BAI03:** gestionar la identificación y construcción de soluciones.
- **BAI04:** gestionar la disponibilidad y la capacidad.
- **BAI05:** gestionar los cambios organizativos.
- **BAI06:** gestionar los cambios de TI.

- **BAI07:** gestionar la aceptación y la transición de los cambios de TI.
- **BAI08:** gestionar el conocimiento.
- **BAI09:** gestionar los activos.
- **BAI10:** gestionar la configuración.
- **BAI11:** gestionar los proyectos.

DSS – Entregar, Dar servicio y Soporte:

- **DSS01:** gestionar las operaciones.
- **DSS02:** gestionar las peticiones y los incidentes del servicio.
- **DSS03:** gestionar los problemas.
- **DSS04:** gestionar la continuidad.
- **DSS05:** gestionar los servicios de seguridad.
- **DSS06:** gestionar los controles de los procesos de negocio.

MEA – Monitorear, Evaluar y Valorar

- **MEA01:** gestionar el monitoreo del rendimiento y la conformidad.
- **MEA02:** gestionar el sistema de control interno.
- **MEA03:** gestionar el cumplimiento de los requerimientos externos.
- **MEA04:** gestionar el aseguramiento.

(Otake, 2019))

El marco de COBIT 2019 se conforma por el siguiente conjunto de publicaciones:

- Marco de referencia COBIT 2019: introducción y metodología.
- Marco de referencia COBIT 2019: objetivos de gobierno y gestión.
- Guía de diseño de COBIT 2019: diseño de una solución de gobierno de información y tecnología
- Guía de implementación de COBIT 2019: implementación y optimización de una solución de gobierno de información y tecnología.
- Implementando el marco de trabajo de ciberseguridad de NIST usando COBIT 2019.

Todas estas publicaciones tienen costo y pueden adquirirse en la siguiente página: https://store.isaca.org/s/store#/store/browse/tiles

Factores de diseño.

El componente que se añadió en COBIT 2019 fueron los factores de diseño, estos impactan en que algunos objetivos sean más importantes que otros, sin importar si son objetivos de gobierno o de gestión.

Se tienen 11 factores de diseño, los cuales se muestran a continuación:

- Estrategia empresarial.
- Metas empresariales.
- Perfiles de riesgo.
- Temas relacionados con I&T (Información y Tecnología).
- Panorama de amenazas.
- Requerimientos de cumplimiento.
- Rol de la TI.
- Modelo de aprovisionamiento de TI.
- Métodos de implementación de TI.
- Estrategia de adaptación de TI.
- Tamaño empresarial.

(ISACA, 2018)

Estos factores de diseño pueden influir en la importancia de un objetivo sobre otro, donde una mayor importancia dignifica un nivel de capacidad mayor.

Etapas de diseño de un sistema de gobierno COBIT 2019

1. **Entender el contexto y la estrategia empresarial.**

Se debe comprender cuales son las metas de la empresa, así como los riesgos y temas pendientes que tiene la organización, los cuales se relacionan con la información y la tecnología.

2. **Determinar el alcance inicial del sistema de gobierno.**

Se debe tomar en cuenta la estrategia empresarial, también tienen que considerarse las metas de la empresa y usar la cascada de metas COBIT, también se tiene que considerar el perfil de riesgo empresarial.

3. **Afinar el alcance del sistema de gobierno.**

Hay que tomar en cuenta el panorama de amenazas, así como el rol que tienen las TI, sus métodos de implementación y sus estrategias de adopción, los modelos de aprovisionamiento, y el tamaño de la empresa.

4. **Concluir el diseño del sistema de gobierno.**

Hay que solucionar los conflictos propios de la priorización, para poder culminar con el diseño del sistema de gobierno.

Gestión del desempeño – capacidad y madurez 2019

El esquema de capacidad de COBIT 2019 está basado en el CMMI, donde los procesos de los objetivos pueden operar en alguno de los niveles de madurez, los cuales van de 0 a 5, este nivel de madurez es la medida que hace referencia a qué tan bien están implementados los procesos. Cada nivel se explica en la tabla 1.2:

Tabla 1.2. Niveles de madurez

Nivel 0	Falta de cualquier capacidad básica, enfoque incompleto para hacer frente al propósito de gobierno y gestión.
Nivel 1	El proceso más o menos cumple su propósito, a través de un grupo de actividades incompletas.
Nivel 2	El proceso cumple su propósito a través de un grupo de actividades básicas completas.
Nivel 3	El proceso cumple su propósito de forma organizada, haciendo uso de activos organizacionales.
Nivel 4	El proceso cumple su propósito, además está bien definido y se mide su desempeño.
Nivel 5	El proceso cumple su propósito y tiene una mejora continua.

(ISACA, 2018)

COBIT 2019 es un marco de gobierno completo, que brinda a las organizaciones flexibilidad para que sean capaces de desarrollar soluciones de gobierno, las cuales se amoldan a los objetivos de la empresa y de los usuarios.

(Chamorro López, 2011; P. González, 2020; Iriarte Medina, 2006; ISACA, 2018; Otake, 2019)

1.2.4. Serie ISO 27000

La serie ISO/IEC 27000 es una familia de estándares de seguridad que fueron desarrollados por la ISO y la IEC, este conjunto de normas establecen una guía de buenas prácticas para el mantenimiento, auditoría, certificación y gestión del SGSI cuyas siglas significan Sistema de Gestión de Seguridad de la Información, estas normas pueden ser usadas por todo tipo de organización, no toma en cuenta si es pública o privada, y tampoco su tamaño

Un SGSI se conforma de políticas, procedimientos e instrucciones para la administración de información que permite a las empresas y organizaciones evaluar riesgos y definir soluciones para eliminarlos o minimizar las consecuencias.

El SGSI se basa el siguiente proceso (véase figura 1.3):

Primero se *planifica* la seguridad de la información, para ello se establece un proceso y se definen los objetivos que se quieren alcanzar, seguido de esto se *implementa* la seguridad de la información en los procesos establecidos, después de ser implementados, estos deben de *operar y mantener* para después *monitorear* los resultados, y *revisar* la efectividad de los mismos teniendo como base los procesos establecidos, finalmente se tiene el proceso de *mejora*, donde los resultados son analizados y se establecen nuevos objetivos.

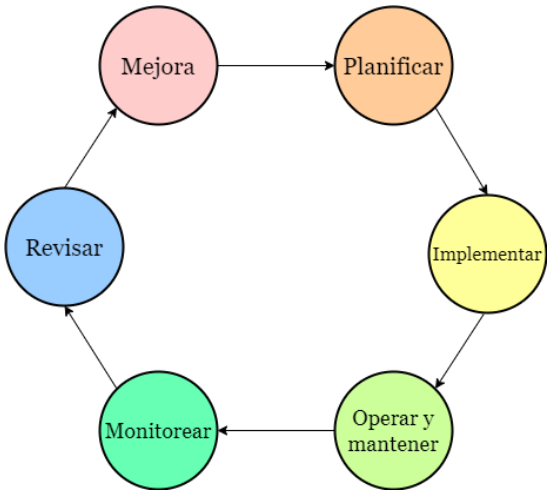


Figura. 1.3. Proceso del SGSI.

Para establecer un SGSI con éxito se deben de tener en cuenta los siguientes principios:

- Hay que considerar la importancia que tiene la seguridad de la información.
- Se deben asignar roles y tareas.
- Tiene que haber compromiso de los altos mandos de la organización y de todos los interesados.
- Hay que hacer evaluaciones de riesgo para definir los controles adecuados para alcanzar niveles de riesgo aceptables.
- Se deben añadir criterios de seguridad, ya que estos son parte fundamental de los sistemas de información.
- Hay que anticiparse a los incidentes de seguridad.
- Se tiene que hacer una evaluación continua para verificar el estado de la seguridad que tiene la información, con el objetivo de hacer las modificaciones necesarias.

Implementar un SGSI debería verse como una estrategia, porque es necesario hacer la integración de criterios de seguridad en los procesos realizados por las organizaciones.

Dentro del estándar ISO/IEC 27000 hay una serie de factores para implementar exitosamente un SGSI:

1. Tomar en cuenta cuales son los objetivos y las políticas de la seguridad de la información, ya que estos deben estar alineados con los objetivos de la organización.

2. La seguridad de la información debe integrar la filosofía de un sistema de gestión en el diseño de los procesos, la operación del sistema y su mantenimiento.
3. Buscar el compromiso de los niveles de administración involucrados, específicamente el compromiso y apoyo de la dirección de la organización
4. Hay que buscar que la evaluación de riesgos garantice que los requisitos para proteger los activos sean comprendidos.
5. El que la implementación del SGSI sea exitoso depende de que tan implicados están los empleados y directivos de manera efectiva, por lo que se debe de capacitar y concientizar a todos los involucrados sobre la importancia que tiene la seguridad de la información para la organización.
6. Se debe de tener un proceso efectivo de gestión de incidentes, ya que estos se producirán en mayor o menor frecuencia así se esté buscando evitarlos, por lo que es importante estar preparados para cualquier incidente que pueda surgir.
7. Hay que evaluar el desempeño del SGSI para obtener una retroalimentación y usarla para mejorar.

En un subtema anterior ya se mencionó que la serie 27000 surgió en 1995 con la norma británica BS-7799, esta norma proporcionaba buenas prácticas relacionadas con la gestión de la información.

La norma BS-7799 constaba de dos partes, la parte uno era la norma BS-7799-1, esta contiene buenas prácticas para las que no se define un sistema de certificación, la parte dos de la norma, la BS-7799-2 se publicó en 1998 y en esta se establecen los requerimientos para que un SGSI pueda ser certificado por una entidad independiente.

En el año 1999 ambas partes de esta norma fueron revisadas, y en el año 2000 solo la primera parte fue adoptada sin cambios por la ISO bajo el nombre de ISO 17799. Dos años después en el año 2002 la segunda parte de la norma fue revisada para adecuarla a la filosofía de las normas ISO de los sistemas de gestión y, para en el 2005 la ISO la adoptó bajo el nombre ISO 27001, al mismo tiempo se hizo una revisión de la ISO 17799 y en el año 2007 fue renombrada como ISO 27002.

En la siguiente tabla, se listan las diferentes normas que conforman la serie ISO 27000:

Tabla 1.3. Normas de la serie 27000

Norma	Publicación	Descripción
ISO/IEC 27000	Primera edición: 01-05-2009 Segunda edición: 01-12-2012 Tercera edición: 14-01-2014 Cuarta edición: febrero 2016	Proporciona una visión general de las normas que componen a la serie 27000, indica el alcance y propósito de cada una de ellas, recopila todas las definiciones de la serie y aporta las bases de la importancia de un SGSI, una introducción al SGSI, así como una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora del SGSI.
ISO/IEC 27001	15-10-2005	Es la norma principal de esta serie, contiene los requisitos para la implantación y certificación de un SGSI, además adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Es certificable
ISO/IEC 27002	01-07-2007	Esta es una guía de buenas prácticas que describe los objetivos de control y controles recomendados para alcanzar los objetivos del SGSI. La última actualización de esta norma es del 15 de febrero de 2022, por lo que consta de 93 controles, de los cuales 37 son relativos a la organización, 8 a las personas, 14 a las instalaciones físicas y 34 a la tecnología. Con esta última actualización, es posible que las organizaciones puedan desarrollar atributos propios para los controles de seguridad, facilitando la integración de la ISO 27000 con otros marcos de gobierno y gestión, teniendo la posibilidad de orientar la implantación de los controles a sectores industriales o sectoriales específicos para las actividades de cada organización. No certificable.
ISO/IEC 27003	Primera edición: 01-02-2010 Actualizada: 12-04-2017	Es una guía que se centra en los aspectos críticos para el diseño e implementación de un SGSI. Se describe un proceso de especificación y diseño desde la concepción hasta la puesta en marcha de los planes de implementación. También se describe el proceso de obtención de aprobación por la dirección para implementar el SGSI. No certificable.
ISO/IEC 27004	Primera edición: 15-12-2009 Revisada: diciembre 2016.	Es una guía para el uso y desarrollo de métricas y técnicas con las que se puede determinar que tan eficaz en un SGSI. No certificable.
ISO/IEC 27005	Primera edición: 15-06-2008 Segunda edición: 01-06-2011. Tercera edición: Julio 2018	Define como se debe realizar la gestión de los riesgos del SGSI, está diseñada para ayudar a la aplicación satisfactoria

		de la seguridad de la información y se basa en un enfoque de gestión de riesgos. No certificable.
ISO/IEC 27006	Primera edición: 01-03-2007 Segunda edición: 01-12-2011 Revisada: 30-09-2015	Especifica los requisitos que deben de cumplir las organizaciones que quieran ser acreditadas para certificar a otras organizaciones en el cumplimiento de la norma ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, esta no es una norma de acreditación por sí misma. No certificable.
ISO/IEC 27007	Primera edición: 14-11-2011 Revisada: 09-10-2017 Segunda edición: 21-01-2020	Es una guía que establece procedimientos para la realización de auditorías internas o externas, cuyo objetivo es verificar y certificar implementaciones de la norma ISO/IEC 27001, además se proporcionan consejos para la selección de auditores. No certificable.
ISO/IEC 27008	Primera edición: 15-10-2011	Define como se deben de evaluar los controles seleccionados en el marco de implantación de un SGSI, con el fin de revisar su adecuación técnica de forma que sean eficaces en la mitigación de riesgos. No certificable.
ISO/IEC 27009	Publicada: 15-06-2016 Revisada: 21-04-2020	Define los requisitos para usar la norma 27001 en algún sector especifico, aquí se especifica como incluir requisitos adicionales, o conjuntos de control a los de la norma 27001. No certificable.
ISO/IEC 27010	Publicada: 20-10-2012 Revisada: 10-11-2015	Define como debe de tratarse la información cuando se comparte entre varias organizaciones o sectores, así como los riesgos que pueden surgir y que se debe hacer para mitigarlos. Se puede aplicar a cualquier forma de intercambio y difusión de información sensible.
ISO/IEC 27011	Publicada: 15-12-2008 Revisada: diciembre 2016	Es una guía para la interpretación de la implementación y gestión de un SGSI en el sector de telecomunicaciones.
ISO/IEC 27013	Publicada: 15-10-2012 Segunda edición: 24-11-2015	Es una guía donde se establecen las normas de integración de las normas ISO/IEC 27001 y de ISO/IEC 20000-1.
ISO/IEC 27014	Publicada 23-04-2013 Actualizada: diciembre 2020	Establece principios para que las organizaciones puedan evaluar, monitorear y comunicar actividades relacionadas con la seguridad de la información
ISO/IEC 27015	Publicada: 23-11-2012	Es una guía de SGSI que está orientada a las organizaciones del sector financiero y de seguros.
ISO/IEC 27016	Publicada: 20-02-2014	Guía de valoración de los aspectos financieros de la seguridad de la información
ISO/IEC 27017	Publicada: 15-12-2015	Proporciona una guía de seguridad para el Cloud Computing

ISO/IEC 27018	Publicada: 29-07-2014 Revisada: 15-01-2019	Proporciona buenas prácticas en controles de protección de datos para los proveedores de servicios de computación en Cloud Computing
ISO/IEC 27019	Publicada: 17-07-2013	Es una guía basada en la norma 27002 para el proceso de sistemas de control vinculados al sector de la energía.
ISO/IEC 27021	Publicada: 31-10-2017	Especifica los requisitos de competencia para los profesionales que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI que cumplan con la norma 27001.
ISO/IEC 27022	Publicada: 11-03-2021	Define un modelo de referencia de procesos para el dominio del SGSI, con el objetivo de guiar a los usuarios a incorporar el enfoque del proceso como se describe en la norma ISO/IEC 27000.
ISO/IEC 27023	Publicada: 02-07-2015	Es una guía de correspondencia entre las versiones del 2013 de las normas 27001 y 27002 como apoyo a la transición de las versiones publicadas en 2005.
ISO/IEC 27030	En fase de desarrollo	Cubrirá la privacidad y seguridad en principios, riesgos y controles aplicables al IoT.
ISO/IEC 27031	Publicada:01-03-2011	Es una guía de apoyo para la adecuación de las TIC de una organización para la continuidad del negocio. Esta norma toma como referencia el estándar BS 25777. No es certificable.
ISO/IEC 27032	Publicada: 16 -07-2012	Proporciona orientación para la mejora del estado de seguridad cibernética, además cubre las prácticas se seguridad a nivel básico en el ciberespacio y establece una descripción general de seguridad cibernética.
ISO/IEC 27033	Parcialmente desarrollada	Es una norma dedicada a la seguridad en las redes.
ISO/IEC 27034	Parcialmente desarrollada	Norma dedicada a la seguridad en aplicaciones informáticas.
ISO/IEC 27035	Publicada: 17-08-2011	Esta norma proporciona una guía sobre la gestión de incidentes de seguridad en la información.
ISO/IEC 27036	Publicada: 24-03-2014	Proporciona una guía de seguridad en las relaciones con proveedores, visión general y conceptos.
ISO/IEC 27037	Publicada: 15-10-2012	Guía que proporciona las directrices para actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias en celulares, tarjetas de memoria, dispositivos electrónicos, sistemas de navegación móvil, cámaras digitales y de video, con el fin de poder ser usadas con valor probatorio en el intercambio de diferentes jurisdicciones
ISO/IEC 27038	Publicada: 13-03-2014	Guía de especificación para la seguridad de la redacción digital

ISO/IEC 27039	Publicada: 11-02-2015 Corrección; 28-04-2016	Guía para la selección, despliegue y operativa de sistemas IDS/IPS.
ISO/IEC 27040	Publicada: 05-01-2015	Guía para la seguridad de medios de almacenamiento.
ISO/IEC 27041	Publicada: 19-06-2015	Guía para garantizar la idoneidad y adecuación de los métodos de investigación
ISO/IEC 27042	Publicada: 19-06-2015	Guía que incluye directrices para realizar el análisis e interpretación de evidencias digitales.
ISO/IEC 27043	Publicada: 04-03-2015	Este estándar desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.
ISO/IEC 27045	En fase de desarrollo	Este estándar cubrirá procesos de seguridad y privacidad en sistemas de big data.
ISO/IEC 27050	Publicada: noviembre 2016	Guía sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis, producción y conceptos generales. Además, es una guía para el gobierno y gestión.
ISO/IEC 27070	En fase de desarrollo	Esta norma establecerá requisitos de seguridad para establecer raíces virtualizadas de confianza en la nube, donde las máquinas virtuales se crean de manera dinámica para proporcionar servicios en la nube.
ISO/IEC 27071	En fase de desarrollo	Esta norma recomendará controles de seguridad para establecer conexiones confiables entre dispositivos y servicios en la nube.
ISO/IEC 27099	En fase de desarrollo	Esta norma ayudará a identificar los requisitos de gestión de seguridad de la información para los proveedores de servicios de confianza de PKI
ISO/IEC 27100	Publicada: 22-12-2020	Proporciona una descripción de la ciberseguridad y de los conceptos relevantes, además, incluirá la forma en la que se relaciona y se diferencia la seguridad de la información, también establece el contexto de la ciberseguridad, sin excluir definiciones procedentes de otros estándares o nuevos términos de uso relacionados.
ISO/IEC 27102	Publicada: 13-08-2019	Proporciona pautas que se tienen que considerar para la contratación de un ciberseguro como opción a tratamiento de riesgos.
ISO/IEC 27103	Publicada: 16-02-2021	Este estándar ayuda a garantizar que se use un conjunto mínimo de conceptos para definir los marcos de ciberseguridad. Los principios de esta norma son: flexibilidad, compatibilidad e interoperabilidad.

ISO/IEC 27550	Publicada: septiembre 2019	Esta norma cubre aspectos de privacidad en ingeniería de sistemas TIC
ISO/IEC 27551	En fase de desarrollo	Esta norma especificará los requisitos para la autenticación de entidad no enlazable basada en atributos.
ISO/IEC 27553	En fase de desarrollo	Especificará los requisitos para la autenticación biométrica en dispositivos móviles.
ISO/IEC 27554	En fase de desarrollo	Brindará orientación sobre el uso de la norma ISO 31000 para evaluar el riesgo relacionado con la gestión de identidad.
ISO/IEC 27555	Publicada: 08-10-2021	Esta norma proporciona un marco para desarrollar y establecer políticas y procedimientos para la eliminación de PII en una organización.
ISO/IEC 27556	En fase de desarrollo	Esta norma brindará un marco centrado en el usuario para manejar la PII en función de las preferencias de privacidad.
ISO/IEC 27570	Publicada: 28-01-2021	Esta norma ofrece orientación sobre la privacidad de los ciudadanos como punto de atención principal en el desarrollo de ecosistemas para las ciudades inteligentes, esta puede aplicarse a cualquier organización, sin importar su tipo o tamaño.
ISO/IEC 27701	Publicada: agosto 2019	Se especifican los requisitos y brinda orientación para establecer, mantener y mejorar un Sistema de Gestión de Información de Privacidad.
ISO/IEC 27799	Publicada: 12-06-2008 Revisión: julio 2016	Esta norma proporciona directrices para apoyar la interpretación y aplicación en el control sanitario para la seguridad de la información sobre los datos de salud de los pacientes.

Información tomada de: https://www.iso27000.es/iso27000.html

Después de revisar las normas que componen a esta serie, es importante saber los beneficios ofrecen las normas de la serie 27000.

Uno de los primeros beneficios es que se tendrá una reducción de los riesgos en la seguridad de la información, además estas normas permiten integrar los objetivos de seguridad y los del negocio, también incluye los procesos, la administración de la organización y la preparación de los colaboradores, fomentando así una cultura de seguridad de la información en la organización.

Otro de los beneficios es que permite adoptar buenas prácticas que son aceptadas internacionalmente, además de que estas se pueden adecuar a las necesidades de las diferentes organizaciones proveyendo confianza a todas las partes interesadas, mejorando así

las expectativas sobre los resultados, además de reducir los costos y mejorar los procesos y servicios.

También, se tiene como beneficio un monitoreo continuo de los riesgos y controles y, con ayuda de las auditorías externas se pueden identificar las áreas donde el sistema presente debilidades para así realizar una mejora.

(Carvajal Herrera, 2013; Chamorro López, 2011; Iriarte Medina, 2006; ISO 27001, s. f., p. 27001; ISO27000, s. f.; Normas ISO, s. f.)

1.3 Esquema de seguridad basado en criterios comunes: perfiles de protección

1.3.1. Definición y propósito

Un perfil de protección abreviado como PP es un conjunto de requisitos de seguridad que cumple con necesidades específicas y que es independiente de la implementación, es decir, que realiza la implementación de los requisitos, sin explicar cómo es que se llevó a cabo, estos se usan como parte de los criterios comunes y pueden estar orientados hacia un objetivo específico o hacia un conjunto de productos de TI.

La función principal de un PP es determinar la efectividad de los protocolos de seguridad, esto lo hace asignando un nivel a cada una de las estrategias, con lo que es posible realizar una evaluación de las medidas de seguridad de una red y de sus componentes individuales.

Los PP no están relacionados con algún producto o sistema, es decir, estos definen las necesidades de un usuario independientemente del producto, por lo regular son reutilizables, es por esto que deben ser genéricos, se componen de dos tipos de requisitos:

- **SFR – Security Functional Requirement, en español Requisitos funcionales de Seguridad:** estos requisitos proporcionan mecanismos que ayudan a cumplir las políticas de seguridad.
- **SAR – Security Assurance Requirement, en español Requisitos de confianza o aseguramiento:** estos requisitos proporcionan una base para tener confianza en que los productos verifican sus objetivos de seguridad, estos se encuentran agrupados en niveles de confianza en la evaluación o EAL, los cuales ya se mencionaron con anterioridad.

El objetivo de la evaluación de los PP es mostrar que dicho PP es completo, consistente y sólido, por lo que podría ser usado para determinar los requerimientos que definen los objetivos de seguridad, por lo tanto, los clientes pueden hacer uso de un perfil de protección para expresar sus políticas de seguridad.

Un objetivo de seguridad es un documento donde se describe el producto o sistema a ser evaluado, también se definen los dispositivos y recursos que usa, así como la documentación y su entorno.

Uno de los principales enfoques que usa un PP es someter al producto o sistema a una serie de amenazas, para ver cómo es que dicho producto gestiona los problemas, manteniendo la integridad, esto va más allá de solo determinar si el sistema está o no correctamente protegido, ya que con este enfoque se identifica la cantidad de recursos que se ocupan para resistir las amenazas y si hay efectos a largo plazo que puedan afectar al objeto de evaluación.

Después de haber explicado lo anterior, se puede decir que un PP es una explicación del producto o sistema que quiere el usuario y de lo que quiere lograr, este documento contiene los requisitos que corresponden a las necesidades del usuario y va dirigido a quienes impulsan su desarrollo, por lo que se solicitan opiniones de los desarrolladores, evaluadores, auditores y reguladores, posteriormente, el usuario entiende la misión de la organización y puede decir que espera y que no del objeto de evaluación.

(Chamorro López, 2011)

1.3.2 Estructura

Después de haber entendido el concepto y propósito de los perfiles de protección, hay que revisar su estructura, que se compone de lo siguiente:

1. **Introducción:** esta parte incluye un resumen ejecutivo, es decir, un resumen de lo que el dueño tiene que ver, asimismo se incluye una explicación clara del problema de seguridad que hay que resolver y de cómo el PP ayuda a resolverlo.
   Hay que tomar en cuenta que es lo único que verán los que toman las decisiones, por lo que hay que asegurarse de que la introducción sea consistente con el contenido técnico del PP.
2. **Descripción del objetivo de evaluación o TOE:** esta parte está enfocada hacia el técnico administrador, por lo que se añaden detalles como que es el TOE y cuál es su entorno. También incluye una descripción funcional, dentro de la cual se incluye además de la definición de las características de seguridad, una descripción de la frontera del TOE, es decir, explica lo que está dentro del alcance del TOE y lo que está fuera de él.
3. **Entorno de seguridad:** el tipo de descripción que se incluye en este apartado facilita la definición de los requerimientos, ya que muestra las hipótesis que se hicieron durante el desarrollo del PP, así como las expectativas que se tienen sobre el entorno y la naturaleza del objeto de evaluación.
4. **Hipótesis:** aquí se deben de identificar las hipótesis, preferentemente hay que asignar un identificador a cada una para simplificar las referencias, también se tiene que identificar el alcance de los requerimientos, estos deben ser relacionados al entorno físico, al personal, a los procedimientos y a la conectividad. Algo importante que se debe señalar es que se debe evitar incluir detalles de las funciones de seguridad dentro de las hipótesis.
5. **Amenazas:** en este apartado, se deben de identificar las amenazas que sean más importantes y los bienes de TI que se quieran proteger, también hay que identificar los métodos de ataque e identificar a los agentes amenazadores.
   Hay que asegurarse de que la descripción de las amenazas sea clara, evitando un traslape entre amenazas, asimismo se debe de especificar su origen. Se deben de incluir

solo las amenazas que ponen en riesgo los bienes de TI, y no solo las amenazas basadas en debilidades o las que surgen por fallas en la implementación del TOE, para facilitar la identificación de las amenazas se sugiere asignar un identificador a cada una.

6. **Políticas de la organización:** hay que definir las políticas o conjunto de reglas que se deben implementar por la TOE y su entorno, también se debe de asignar el nivel de garantía general requerido, e igual que en puntos anteriores, se sugiere asignar un nombre o etiqueta a cada una de las políticas para identificarlas más rápido.
7. **Objetivos:** en este punto se debe de identificar lo siguiente:
    a. Cómo es que se hará frente contra las amenazas.
    b. Determinar cual es la naturaleza de los requerimientos, así como el nivel de efectividad que se espera.
    c. Identificar el tipo de relación que hay entre las amenazas, las políticas y el objetivo, la cual puede ser muchos a uno o uno a muchos.

    Si a este punto ya se conocen los requisitos funcionales de seguridad, se debe de identificar un objetivo de seguridad para cada uno de los requisitos funcionales, esto con la finalidad de facilitar el mapeo de los objetivos a los requisitos. También debe de quedar claro si el objetivo es de tipo preventivo, detectivo o correctivo. Finalmente, para identificar con mayor facilidad los objetivos a cada uno se le debe de asignar un nombre o etiqueta.
8. **Requerimientos:** la actividad esencial de este apartado es determinar qué objetivos le posibilitarán al TOE y a su entorno funcionar de manera segura y también los que le permitan al entorno garantizar la seguridad del TOE, por lo que de aquí se definen dos tipos de requerimientos, los requerimientos funcionales y los requerimientos de garantía. Los funcionales hacen referencia a lo que requiere el TOE para que funcione de manera segura, mientras que los de garantía indican todo aquello que garantiza que el TOE es seguro y que por lo tanto el usuario considera confiable.

    Los requerimientos de garantía se seleccionan teniendo como base el valor de los activos que se quieren proteger, también hay que tomar en cuenta los riesgos a los que se exponen dichos activos, costos probables y tiempos disponibles.

    Los requerimientos de seguridad del entorno de TI deben ser definidos con un grado de abstracción apropiado en el PP, esto para evitar que se definan en términos de la implementación específica.

    Dentro de este apartado también hay que indicar las funciones que debe realizar el TOE y las funciones que debe realizar su entorno, tanto en conjunto como por separado, también se debe de dar un margen a lo que haga el TOE, dando la flexibilidad en el diseño.

    Se deben dar los motivos de confianza o garantías, las cuales dependen del desarrollador y del operador, también hay que definir las medidas de evaluación o auditoría, las cuales están basadas en el PP.

También se lleva a cabo la selección y asignación de los componentes funcionales del PP, esto para evitar dar una solución que sea inconsistente con los objetivos de seguridad.

9. **Justificación o explicación:** es un documento aparte, en él se muestra por qué el PP está completo, es correcto y consistente.
   Se tiene que hacer un mapeo de los objetivos contra los riesgos, las políticas organizacionales e hipótesis, donde se muestre que cada riesgo, política e hipótesis está cubierta por al menos un objetivo de seguridad, además se debe añadir una explicación donde se justifique el porqué de los objetivos señalados.
   Otro mapeo que hay que hacer es el de los requisitos funcionales de seguridad con los objetivos de seguridad, se tiene que mostrar que cada uno de los objetivos está cubierto por un requerimiento funcional, de igual forma se tiene que añadir una justificación del porqué son adecuados los dichos requerimientos.
   También se debe demostrar que los requisitos no están en conflicto, es decir, se tiene que demostrar que un requisito funcional no permite que otro de los requisitos sea evitado, alterado o desactivado.

(Chamorro López, 2011)

1.4 Servicios de seguridad

Desde hace muchos años, la humanidad ha vivido conectada a algún tipo de red, por lo que cada vez aumenta la complejidad para proteger la información. Todos los elementos que integran un sistema están expuestos a sufrir algún tipo de ataque, por lo que es importante saber protegerlos correctamente para minimizar los daños que puedan ocurrir.

La seguridad informática, tiene como objetivo primordial garantizar la confidencialidad, disponibilidad e integridad de la información, estos tres elementos son comúnmente conocidos como la "Triada CID" (véase figura 1.4), los cuales deben de trabajar en conjunto para mantener seguro a los sistemas informáticos, por lo que hay que tenerlos en cuenta al momento de diseñar alguna estrategia de seguridad.

Figura 1.4. Triada CID

(Leal, 2012)

1.4.1. Confidencialidad

En muchas situaciones es necesario proteger información para que solo accedan a ella las personas autorizadas. La confidencialidad es un servicio de seguridad donde se busca prevenir el acceso no autorizado sin importar si es o no intencional y cuidar del acceso no autorizado a personas, sistemas o procesos.

Este servicio de seguridad también toma mucha importancia cuando se trata de transmitir datos que son muy sensibles, si una organización llega a fallar en la confidencialidad de la información podría traerle problemas legales, además de pérdida de credibilidad.

La confidencialidad es un servicio de seguridad que va de la mano con la autenticación, puesto que, para mantener a salvo la información sería necesario que quien quisiera acceder a ella se

autenticara de manera exitosa. Por ejemplo, una persona, sistema o proceso requiere acceder a información almacenada, para mantener su confidencialidad, quien accede debe comprobar que tiene la autorización necesaria, esto lo hace por medio de una autenticación, donde dependiendo del resultado se sabe si tiene o no los permisos necesarios.

1.4.2. Integridad

Este servicio de seguridad se refiere a la confiabilidad de la información o recurso que se busca proteger, este servicio consiste en evitar que haya algún tipo de modificación no autorizada, como puede ser el borrado total o parcial, copiar la información en otro dispositivo, o reordenarla sin previa autorización, esto puede ser durante su transmisión o mientras se encuentra almacenada.

La integridad hace referencia a dos conceptos, uno sería la integridad de los datos, es decir, el volumen de la información, y el otro hace referencia a la integridad del origen, ésta se refiere a la fuente de donde proviene la información, por lo que, si esta se ve alterada, la información que surja después va a ser incorrecta, además de perder exactitud, credibilidad y confianza.

Un ejemplo de esto es cuando se difunde información mediante un medio impreso, al ser impreso se está manteniendo la integridad de los datos, pero si la fuente de donde fueron tomados es errónea ya no se está manteniendo la integridad de origen.

Otro ejemplo puede ser el envío de una carta mediante un servicio postal, el sobre que contiene la carta va totalmente sellado, con la finalidad de que nadie en el transcurso al destino lo abra, si este sello al llegar al destino se encuentra roto se puede decir que fue abierto en el transcurso con la posibilidad de haber sido alterado, por lo que fue violada la integridad de dicha carta, en cambio, si el sobre se encuentra debidamente sellado se puede tener la garantía que el contenido sigue siendo íntegro y no hay algo de lo que preocuparse.

Si no se tiene un buen cuidado en la integridad de la información se podrían tener graves consecuencias, que pueden acabar en fraudes e incluso dar paso a algún tipo de ataque.

1.4.3. Disponibilidad

Este servicio de seguridad hace referencia a que el sistema esté operando de manera continua, con el objetivo de que los usuarios autorizados tengan acceso a la información en el momento en que lo necesiten. La disponibilidad suele expresarse como un porcentaje, este indica la cantidad de tiempo que un sistema se encuentra activo en un periodo determinado.

La disponibilidad tiene como objetivo impedir que haya interrupciones no autorizadas o no controladas de los recursos. Si se tienen fallos en este servicio de seguridad se pueden acarrear

pérdidas en la productividad y credibilidad de la organización, porque al perder la disponibilidad ya no se podrían satisfacer los requisitos.

Los datos deberían ser accesibles así se presenten cortes de corriente, accidentes e incluso ataques, esto se vuelve muy importante, porque al perder disponibilidad se pueden provocar reacciones en cadena que afecten otras operaciones, con lo anterior, se vuelve importante tener presentes la necesidad de contar con medidas de protección que garanticen que los datos estarán disponibles ante cualquier percance.

El servicio de disponibilidad debe garantizar que todo sistema, proceso o persona autorizada pueda acceder a la información cuando se desee y tantas veces como se requiera, sin embargo, es importante destacar que el estar los servicios disponibles las veinticuatro horas del día, los trescientos sesentaicinco días del año va a depender directamente de las políticas de la empresa u organización que preste esos servicios.

Lograr la disponibilidad al 100% es sumamente complicado ya que suele ser muy caro, sin embargo, hay sistemas que por el servicio que ofrecen se requiere que estén funcionando las veinticuatro horas del día, este concepto se conoce como alta disponibilidad.

La alta disponibilidad describe a aquellos sistemas donde se trata de evitar el tiempo de inactividad, aseguran que el periodo de rendimiento sea más alto de lo normal y que el sistema siga funcionando aun cuando se presenten condiciones extremas como un ataque o corte de energía.

Un sistema puede tener el 90% de disponibilidad al año y podría pensarse que este porcentaje es bastante bueno, sin embargo, un sistema con 90% de disponibilidad se encuentra aproximadamente 36.5 días de tiempo de inactividad no planificada al año.

Otro sistema puede ofrecer un porcentaje de disponibilidad del 99%, lo cual, significa que tendría 3.65 días de inactividad no planificada al año, sin embargo, a pesar de ser poco el tiempo inactivo no es considerado un sistema de alta disponibilidad, los sistemas que si entran en esta categoría son aquellos que ofrecen un porcentaje mayor o igual al 99.5%, tomando lo anterior en cuenta, se tiene que un sistema que ofrece un porcentaje de 99.9% se encuentra inactivo 8.76 horas al año, lo cual ya es realmente poco, pero esto no termina aquí, ya que hay sistemas que pueden ofrecer el 99.99% de disponibilidad, lo cual indica que su tiempo de inactividad no planificada es de 52.5 minutos al año.

Sin embargo, hay sistemas que ofrecen una disponibilidad de 99.999%, lo cual significa que su tiempo de inactividad es de 5.26 minutos al año, este tipo de sistemas es considerado un sistema tolerante a fallos, sin embargo, lograr este nivel de disponibilidad implica grandes costos.

Adicionalmente a la triada CID existen tres elementos más que hay que tener en cuenta para garantizar la seguridad de un sistema, estos elementos son la autenticación, no repudio y el

control de acceso, estos tres elementos y la triada CID son mejor conocidos como *servicios de seguridad*, los cuales mejoran mucho la seguridad de un sistema, ya que están dirigidos a evitar ataques de seguridad, por lo que se pueden usar uno o más mecanismos para mantener seguro el sistema y que éste funcione de la manera que se espera.

1.4.4. Autenticación

Con este servicio se busca verificar la identidad de usuarios, sistemas y procesos. En cuanto a usuarios se refiere existen varios métodos de autenticación:

1. **Por lo que se sabe:** se pueden incluir las contraseñas o preguntas de seguridad.
2. **Por lo que se tiene:** un ejemplo puede ser una tarjeta magnética.
3. **Por lo que uno es:** se incluye la verificación mediante datos biométricos, como el reconocimiento de huellas dactilares o reconocimiento de iris.

Nada limita a una organización a usar un solo método de autenticación, al contrario, entre más métodos se usen, las probabilidades de que la autenticación sea correcta aumentan.

El método más usado para realizar una autenticación es el uso de contraseñas, sin embargo, la seguridad que proporciona este método depende de las características que tenga la contraseña a usar, por ende, entre más robusta sea se tendrá una mayor seguridad, además las contraseñas usadas deben ser confidenciales, por lo que no se recomienda anotarla en un papel o dejarla visible fácilmente ya que eso vuelve vulnerable al usuario, porque otra persona puede ver la contraseña y autenticarse, haciéndose pasar por alguien que no es.

La autenticación puede ser directa o indirecta, así como unidireccional o mutua:

- **Directa:** solo intervienen las partes interesadas en la autenticación.
- **Indirecta:** hay una tercera persona que valida la identidad de quien o quienes se están autenticando.
- **Unidireccional:** basta que solo se autentique una de las partes.
- **Mutua:** se necesita que ambas partes se autentiquen.

Como se mencionó con anterioridad, también puede realizarse una autenticación entre sistemas y procesos, para esto se hace uso de herramientas criptográficas, las cuales proporcionan la seguridad necesaria para para la transmisión de datos a través de la red.

Hay tres tipos de criptografía que se pueden usar, criptografía de clave secreta, criptografía de clave pública y las funciones hash.

- **Criptografía simétrica o de clave secreta:** este es un sistema de cifrado antiguo que consiste en que el emisor y el receptor cifren y descifren la información haciendo uso de una clave que ambos conocen.

- **Criptografía asimétrica o de clave pública:** este sistema de cifrado usa dos claves, una para cifrar y otra para descifrar. Este se usa principalmente para la autenticación e intercambio de claves, el emisor con la clave pública del receptor cifra la información y el receptor para descifrar la información recibida hace uso de su clave privada, por lo que se considera más seguro.
- **Funciones hash:** este tipo de cifrado hace uso de transformaciones matemáticas que cifran los datos de manera única, se dice que la creación de un hash es un proceso que va en un solo sentido, ya que es muy complicado realizar el descifrado una vez que el hash está formado, por lo que es un sistema de cifrado muy seguro. Las funciones hash se usan principalmente para preservar la integridad de la información.

1.4.5. No repudio

Este servicio de seguridad proporciona protección durante la comunicación, pues evita que el emisor niegue haber enviado algún mensaje o que el receptor niegue haberlo recibido. Asimismo, garantiza que si se ha ejecutado alguna acción por parte de un usuario, sistema o proceso la acción quede debidamente registrada sin que se pueda negar su ejecución. Dicho de otra manera, el no repudio es la capacidad de demostrar la contribución de todas las partes dentro de la comunicación

Para realizar la implementación de este servicio se puede hacer uso de firmas digitales, técnicas de cifrado de clave pública y en caso de usar cifrado de clave secreta se usa una tercera parte que verifique las identidades, por ejemplo, los certificados digitales.

1.4.6. Control de acceso

Este servicio de seguridad permite que los datos, recursos o servicios que un usuario genera no puedan ser accedidos por otro a menos que sea solicitado por el dueño. El usuario que quiere tener acceso a dicha información debe de pasar primero por un método de autenticación o identificación exitoso para que se le permita el acceso a los datos que necesita.

Todos los objetos de un sistema deben de estar protegidos con mecanismos de control de acceso y se deben de establecer diferentes niveles de acceso acorde a los usuarios, sistemas o procesos para permitirles su acceso.

Por ejemplo, un usuario puede solo tener el acceso en modo lectura a un archivo, lo que significa que solo tiene los permisos necesarios para visualizar el contenido del archivo y no tiene permisos para modificarlo, mientras que otro usuario podría tener permisos de lectura y escritura, lo que además de permitirle visualizar el archivo tiene los permisos necesarios para realizar modificaciones sobre el mismo.

En el control de acceso se ven implicadas diferentes partes, no únicamente el departamento de seguridad, si cada uno de los departamentos gestiona los controles de acceso de manera independiente pueden ocurrir problemas de seguridad, por lo que una buena opción es integrar el control de acceso con los sistemas y procesos de la organización.

La gestión de identidad y accesos conocido como IAM que deriva del inglés Identity and Access Management, es un proceso que permite administrar un conjunto de identidades y los privilegios asociados a cada una de ellas, dentro de una organización el IAM puede ser un producto único o una combinación de procesos que brinda control sobre los datos de la organización a los que pueden acceder los usuarios de manera individual.

Un ejemplo de este proceso sería cuando los derechos de acceso de un empleado son modificados al mismo tiempo que deja de laborar en la organización o cambia su puesto de trabajo, esto para mantener los niveles de seguridad. Para garantizar que este proceso se produzca automáticamente es necesario que la base de datos que gestiona los accesos esté vinculada a la base de datos del área de recursos humanos, para que al momento de que haya modificaciones en los derechos de acceso estos se vean reflejados en la base de datos de gestión.

Otro ejemplo que se tiene del control de acceso son las ACL, ya que estas permiten o deniegan el acceso a los usuarios, basándose en sus características, como, por ejemplo, el área a la que este pertenece dentro de la organización.

Integrar el control de acceso a los sistemas y procesos de una organización trae consigo varias ventajas como la coherencia en los procedimientos, procesos más eficaces, y también una mejora en la productividad.

(Carvajal Herrera, 2013; Delgado Avenia, 2017; López Barrientos & Quezada Reyes, 2019; Lucana Mamani, s. f.; Rentería Echeverry, s. f.; Romero Castro et al., 2018)

Tema 2. Amenazas y vulnerabilidades

2.1. Amenazas

2.1.1. Definición

Una amenaza puede definirse como la *posibilidad* de que ocurra de un evento accidental o intencionado que ponga en riesgo la seguridad de un sistema. Estas pueden provocar daños materiales y pérdidas financieras dentro de la organización.

De manera muy general, las amenazas se pueden clasificar en cinco tipos: las que derivan de sucesos naturales, como los terremotos, huracanes, incendios, inundaciones, solo por mencionar algunos, las que provienen de la actividad humana, como guerras, terrorismo, y explosiones, entre otras, también se tienen amenazas de tipo lógico, tipo físico y los errores en la red.

La seguridad informática busca proteger los sistemas de información, por lo que, si una amenaza llegara a efectuarse, ocurriría un ataque (tema 3) y se podrían tener diversas consecuencias, como la interrupción de un servicio, modificación o eliminación de datos y robo de equipo.

2.1.2. Fuentes de amenaza

Como ya se mencionó anteriormente, las amenazas se pueden clasificar en cinco tipos (véase figura 2.1):

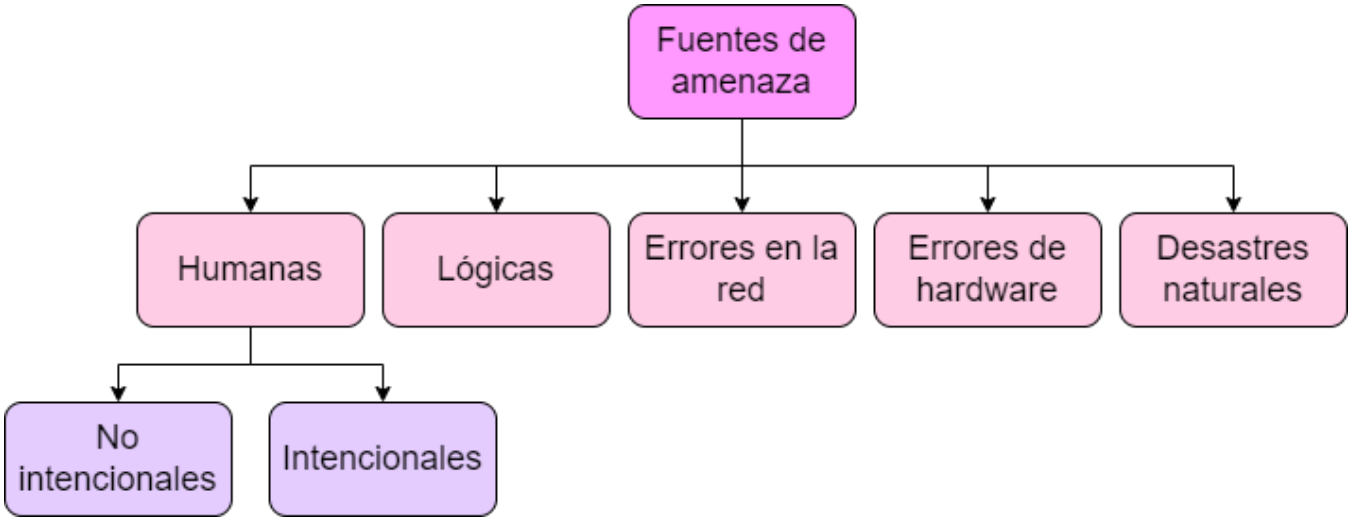


Figura 2.1. Fuentes de amenaza.

A continuación, se explicará a detalle cada una de estas fuentes:

2.1.2.1 Desastres naturales

Este tipo de amenazas son las que se crean por factores ambientales y geográficos, estas no afectan únicamente a la información que está almacenada en los sistemas, ya que también ponen en riesgo a los equipos físicamente.

Entre las principales fuentes de amenazas originadas por desastres naturales se encuentran:

- **Incendios:** estos pueden ocasionarse por muchos factores, entre ellos el uso incorrecto de combustibles o fallas en la instalación eléctrica**.** Para evitar este tipo de desastres se sugiere seguir ciertas recomendaciones, como que el área donde se encuentren los equipos no esté cerca de áreas inflamables o que se haga uso de materiales resistentes al fuego, asimismo se recomienda llevar a cabo la instalación de sistemas contra incendios.
- **Inundaciones:** estos se pueden provocar por la falta de drenaje natural o artificial, incluso pueden ser ocasionados por filtraciones al momento de apagar algún incendio en un piso superior, o por una mala elección de lugar dentro del edificio. Para evitar este tipo de amenaza se pueden seguir ciertas recomendaciones, como no instalar los equipos en lugares cercanos a un baño o sótano, donde el riesgo es mayor, así como la instalación de un techo impermeable para evitar filtraciones de pisos superiores. Asimismo, seguir con las recomendaciones de los gobiernos estatal y federal para las zonas que tienen un alto riesgo de inundaciones.
- **Terremotos:** este tipo de fenómenos físicos son impredecibles, por lo que en caso de ocurrir alguno las organizaciones deberían estar preparadas. En el peor de los casos, este tipo de desastres puede traer una pérdida total de los equipos, por lo que las organizaciones deben de tener respaldos de la información en sitios foráneos o en una nube para garantizar que ante un desastre se cuente en todo momento con la información disponible.

Hay que recordar que no son las únicas amenazas originadas por desastres naturales que pueden ocurrir, otras que pueden comprometer la seguridad del sistema son tormentas, tornados y huracanes, solo por mencionar algunos.

Es importante que se tenga mucho cuidado en la elección del lugar de instalación de los equipos, se puede hacer uso de diferentes estándares que promuevan la seguridad física de los mismos y complementar con el diseño de políticas que ayuden a salvaguardar la integridad física del sistema.

2.1.2.2 Humanos

Las amenazas de este tipo pueden ser causadas de manera accidental o intencionada, sin embargo, causan enormes pérdidas a las organizaciones. Dentro de este tipo de amenazas se encuentran:

- **Hackers:** un hacker es una persona que tiene conocimientos sólidos en el área de la informática, quien es capaz de hacer modificaciones al sistema, dichas modificaciones pueden dañarlo o bien, alertar de las probables amenazas y vulnerabilidades que pueda tener. Los hackers penetran a los sistemas por diferentes motivos, el cual determina la clasificación a la que pertenecen:
    - **Script kiddies:** este término hace referencia a quienes carecen del conocimiento necesario para realizar hacking, sin embargo, se autonombran *hackers.* Sus ataques los realizan usando herramientas que descargan de internet, esto debido a que no tienen el conocimiento necesario para realizar sus propias herramientas, esto a su vez provoca que no comprendan los efectos reales de sus acciones, y a su vez dejan rastros que revelan su identidad, muchas veces al descargar los virus o kits de ataque que encuentran en internet terminan dañando sus propios dispositivos.

      El objetivo principal de los script kiddies es impresionar a sus amigos, así como ganar reconocimiento y demostrar que son capaces de realizar ataques.
    - **White hat:** penetran en los sistemas con previa autorización con el fin de encontrar debilidades para mejorar su seguridad, también se les conoce como hackers éticos, usan sus habilidades para fines éticos o legales.
    - **Grey hat:** penetran el sistema para descubrir vulnerabilidades y en algunos casos publican en internet lo que encontraron para que otros le saquen provecho.
    - **Black hat:** aprovechan las vulnerabilidades que encuentran en el sistema para obtener un beneficio económico o político.

  Como ya se mencionó, los hackers poseen un gran conocimiento en informática, como formatear un equipo, instalar un sistema operativo o hacer uso de Linux, ya que en este sistema operativo es donde se encuentra la mayoría de software de pentesting, adicionalmente, contar con conocimientos de redes para usarlos a su favor, de igual manera es importante que tengan habilidades dentro de la programación, para poder realizar sus propios virus y saber explotar las vulnerabilidades de las bases de datos.
- **Ingeniería social:** este tipo de atacante usa sus habilidades sociales y de interacción para obtener información de su interés, pueden hacerse pasar por alguien de confianza por lo que es capaz de engañar a otras personas y así obtener la información que necesita.

  Por ejemplo, hay un atacante intentando penetrar en un sistema mediante el uso de ingeniería social, primero construye una relación de confianza entre las personas alrededor del sistema que quiere atacar para acumular información del entorno de dicho

sistema, es decir, nombre de los empleados junto con datos personales, como email, número de teléfono, entre otros datos más. Después de haber conseguido información útil que considere suficiente, el atacante se aprovecha de la confianza que le tienen los demás para obtener información que le permita ingresar al sistema más fácilmente para realizar su ataque, una vez hecho esto, el delincuente debe de desaparecer sin dejar rastro o algo que deje al descubierto su verdadera identidad.

- **Ingeniería social inversa:** en este tipo de ingeniería social, el atacante pone una trampa para que algún usuario caiga en ella, este tipo de trampa puede ser phishing o distribución de malware, solo por mencionar algunos, después de que el usuario cae en la trampa del atacante, este sabotea el sistema y después sale a escena, apareciendo como un técnico o alguien de confianza que ofrece ayuda para solucionar los problemas en el sistema, los usuarios al creer que es alguien en quien pueden confiar proporcionan las contraseñas e información necesaria que el atacante pida.
- **Terroristas:** esta clasificación engloba a todo aquel que busca causar pánico o terror a través de los sistemas informáticos.
- **Robo:** la información que contienen los equipos puede ser copiada a dispositivos no autorizados, también se pueden robar físicamente los dispositivos, por lo que aplicar medidas de seguridad se vuelve importante para cuidar su integridad, entre estas medidas se encuentra el control de acceso, autenticación y uso de contraseñas, es decir, se requieren medidas de seguridad físicas y lógicas.
- **Personal interno:** regularmente se tiene la confianza en el personal que labora en la organización, por lo que se pensaría que serían incapaces de hacer algo que vaya a causar daño, sin embargo, el personal podría ser una amenaza para el sistema, ya que pueden causarle daños de manera accidental o intencionada. En el caso de ser de manera accidental puede deberse a la falta de conocimiento de las políticas que maneja la empresa o a la falta de programas de capacitación. En tanto que, si es intencional, se considera importante que las empresas realicen periódicamente evaluaciones de confiabilidad al personal cercano a la información sensible.
- **Ex – empleados:** puede darse el caso de que los ex – empleados causen daños al sistema por algún descontento con la organización, pueden aprovecharse de las debilidades que saben que el sistema tiene y provocar daño como un tipo de venganza hacia la organización para la que antes laboraban. Por lo que es importante que cuando alguien deja la empresa se le deban cancelar todas sus credenciales.
- **Intrusos remunerados:** se trata de personas que reciben una remuneración económica de una tercera persona, con el objetivo de robar información o de perjudicar la reputación de la organización.

2.1.2.3 Lógicas

Este tipo de amenazas pueden tomar forma de algún software que dañe el sistema de manera intencionada, como el malware, o que lo dañe por error, como en el caso de los bugs, los cuales son errores o defectos en el software estos provocan que un programa no funcione de la manera en que debería hacerlo.

Un malware es un software diseñado para interrumpir las operaciones de las computadoras, con el fin de acceder a los sistemas informáticos sin que el usuario tenga conocimiento de ello, es importante resaltar que el malware puede cifrar o eliminar datos, modificar o desviar las funciones básicas del equipo e incluso espiar la actividad de los usuarios.

Las amenazas lógicas pueden ser muy diversas, entre los principales tipos de malware se encuentran:

- **Virus:** los virus son códigos que se insertan en un fichero ejecutable, el cual tiene por nombre huésped, al mismo tiempo que el huésped es ejecutado se ejecuta también el virus, insertándose a sí mismo en otros programas.
- **Gusanos:** este es un programa que tiene la capacidad de ejecutarse y replicarse a sí mismo por las redes, también pueden ser portadores de virus o aprovechan los bugs del sistema para dañarlo.
- **Caballos de Troya:** estas son instrucciones que van ocultas en un programa, de tal manera que cuando se ejecuta hace creer al usuario que está realizando sus tareas correctamente, sin embargo, también se están ejecutando las instrucciones escondidas a espaldas del usuario, como puede ser el robo o destrucción de datos.
- **Adware:** este tipo de malware tiene dos propósitos, uno de ellos es mostrar publicidad al usuario para que los creadores del adware obtengan ganancias y la otra es recopilar información personal de los usuarios, como contraseñas, datos bancarios, datos de navegación, entre otros. El adware puede instalarse mientras se descargan aplicaciones de sitios web de poca confianza, mientras se navega por páginas web no seguras e incluso cuando se instalan extensiones en el navegador.
- **Spyware:** este es un software diseñado para recopilar datos de los dispositivos y reenviarlos a otra persona, esto con conocimiento y sin consentimiento del usuario. El spyware puede consumir muchos recursos del dispositivo, lo que hace que el dispositivo comience a funcionar más lento, asimismo puede sobrecargarlo, ocasionando daños permanentes.

2.1.2.4 Errores de hardware

Un error de este tipo hace referencia a errores en el funcionamiento de los componentes de hardware de un sistema informático, como la tarjeta gráfica, la fuente de alimentación, memoria RAM, placa base, entre otros. Estos errores se pueden clasificar en:

- **Errores corregidos:** este tipo de errores son los que se corrigen por el mismo hardware o por el firmware en cuanto el sistema operativo es notificado con una condición de error.
- **Errores no corregidos:** estos errores son los que el hardware o firmware no pueden corregir cuando se notifica al sistema operativo del error. Estos se subdividen en:
    - **Errores fatales:** son errores en donde se determina que el hardware no se puede recuperar. Al producirse errores de este tipo el sistema operativo genera una comprobación de errores para contener el error.
    - **Errores no fatales:** son errores no corregidos a partir de los cuales el sistema operativo intenta recuperarse tratando de corregir el error, si este no se puede corregir, el sistema operativo genera una comprobación de errores para contenerlo.

Los errores de hardware más comunes son los siguientes:

- **Errores en tarjeta gráfica:** este tipo de errores puede ocasionar que la computadora no arranque correctamente. Entre los fallos que se pueden presentar se encuentra que la computadora encienda, pero no se visualice nada en el monitor, o que salgan líneas extrañas, incluso puede pasar que la computadora haga sonidos no habituales al encenderse.
- **Errores en la fuente de alimentación:** este es uno de los errores más comunes, se presentan cuando dicha fuente no proporciona el voltaje necesario a la placa base para que la computadora pueda prender, otro error relacionado a la fuente de alimentación es cuando no proporciona voltaje de manera estable por lo que se presenta inestabilidad en otros componentes, otro error que se podría presentar es cuando la fuente se apaga de manera repentina, provocando a su vez que se apague la computadora y se pierdan los datos con los que se estaba trabajando.
- **Errores en la memoria RAM:** este tipo de errores causa inestabilidad al equipo en general, dependiendo de los sectores de memoria que se hayan dañado, si la memoria RAM se encuentra muy dañada la computadora no prendería.
- **Errores en el microprocesador:** estos se producen generalmente por un sobrecalentamiento en el microprocesador, provocando que el equipo se apague.
- **Errores en el disco duro:** estos errores pueden ser lo más delicados y que más daño causen, debido a que la información se encuentra almacenada en el disco duro, por lo que es importante realizar respaldos de manera regular. Los errores en los discos duros pueden ser lógicos o físicos, los lógicos hacen referencia a errores en el sistema de

archivos, mientras que los errores físicos pueden presentarse por fallos en alguno de los componentes que conforman el disco duro.

Los errores de hardware pueden traer consigo pérdida de información, mal funcionamiento del sistema y en el peor de los casos una pérdida total del dispositivo, por lo que hay que estar alerta para no perder información importante.

Realizar mantenimiento a los dispositivos toma mucha importancia, este engloba acciones que permiten cuidar o reemplazar oportunamente los componentes. Algunas de las acciones que se tienen que llevar a cabo se encuentran:

- Limpieza de componentes.
- Desfragmentación de discos duros.
- Escaneo de errores en el sistema.

Hay dos tipos de mantenimiento de hardware, el mantenimiento preventivo y el correctivo:

- **Mantenimiento preventivo:** permite anticipar el deterioro de dispositivos, busca mantener los componentes en óptimo estado para alargar su vida útil, además permite detectar oportunamente cuando algún componente necesite ser reemplazado, para esto se toman acciones estratégicas, como la limpieza constante de los dispositivos, esto para evitar el sobrecalentamiento debido a polvo o suciedad que se pudiera acumular, dentro de este tipo de mantenimiento también se incluye el mantener los dispositivos a una temperatura donde puedan funcionar adecuadamente.
  Además del mantenimiento físico del hardware se tienen que tomar acciones sobre el sistema, es decir, tomar acciones para las partes no físicas, ya que esto también influye directamente en el alargamiento de la vida útil del hardware. Esto hace referencia a verificar que el sistema se encuentre actualizado para contar con los parches de seguridad, asimismo hay que verificar que los controladores estén actualizados, e incluso es necesario eliminar el software que ya no sea de utilidad, también es importante instalar y mantener actualizados los antivirus o antimalware, esto porque un virus o malware potente puede dañar por completo componentes de hardware.
- **Mantenimiento correctivo:** este tipo de mantenimiento hace referencia al proceso de reparación o cambio de los componentes de hardware cuando estos dejan de funcionar de manera óptima. Hacer esto puede traer diversos problemas, entre ellos la pérdida de información, incluso puede verse afectada la disponibilidad.

Realizar mantenimiento resulta importante, para detectar fallas o errores por lo que es recomendable realizar mantenimiento preventivo en vez de mantenimiento correctivo, ya que esto, además, ayuda a disminuir los costos dentro de la organización.

2.1.2.5 Errores en la red

Este tipo de amenaza se presenta cuando hay fallas en la red, estas pueden ocasionarse por un mal diseño, lo que puede provocar que la red se sature. El ancho de banda es repartido de manera igualitaria entre todos los dispositivos que se encuentren conectados, por ende, entre más dispositivos haya el intercambio de información será más lento, por lo que puede llegar el momento en el que la comunicación se vuelva imposible y el sistema quede bloqueado, esto puede acarrear pérdida de información o que usuarios no autorizados accedan a información que no deberían acceder.

La información a través de las redes puede viajar a través de dos medios de transmisión, los medios guiados y los no guiados, por lo que se pueden presentar errores de red en el aspecto físico, en los medios no guiados podría presentarse interferencia, mientras que con los medios guiados podrían presentarse fallas o daños en el medio que afecten la integridad de los datos.

Adicionalmente, se pueden presentar errores de red en el aspecto lógico, dentro de este tipo de errores se encuentran las amenazas de monitorización, ataques de autenticación, engaños de DNS (Domain Name Server o Sistema de Nombres de Dominio), entre otros, que de igual manera perjudican la integridad de los datos de la red.

Hay que recordar que la seguridad informática tiene como objetivo mantener la integridad, disponibilidad y confidencialidad de los sistemas, por lo que es importante tener una buena estructura de seguridad para evitar que las amenazas se lleven a cabo y que así la información se encuentre debidamente protegida, para evitar pérdidas materiales o económicas que puedan afectar gravemente a la organización.

(Ciberseguridad, s. f.-c; Delgado Avenia, 2017; Gómez, 2015; Learn Microsoft, 2023; Ptolomeo UNAM, s. f.-a, s. f.-b; Romero Castro et al., 2018; Tarazona T, 1969; Vélez Martínez, s. f.)

2.2. Vulnerabilidades

2.2.1. Definición

Una vulnerabilidad hace referencia a una *debilidad* que puede explotarse para causar daño o pérdidas a un sistema, estas pueden aparecer en el hardware, software e incluso en el sistema operativo. Las vulnerabilidades se consideran un elemento interno del sistema, en este sentido, los administradores y usuarios son quienes deben de detectarlos, evaluarlos y reducirlos.

Una vulnerabilidad es el resultado de bugs o fallas en el diseño de un sistema, las cuales pueden causar daños y producir pérdidas a una organización.

2.2.2. Tipos de vulnerabilidades

Es importante que las organizaciones identifiquen los puntos débiles que tienen, para así tomar medidas de seguridad correctas y reducir en la medida de lo posible las vulnerabilidades que se puedan presentar y que en dado caso de ocurrir se tenga una solución rápida para evitar que el sistema deje de funcionar por completo.

Las vulnerabilidades se clasifican de la siguiente manera:

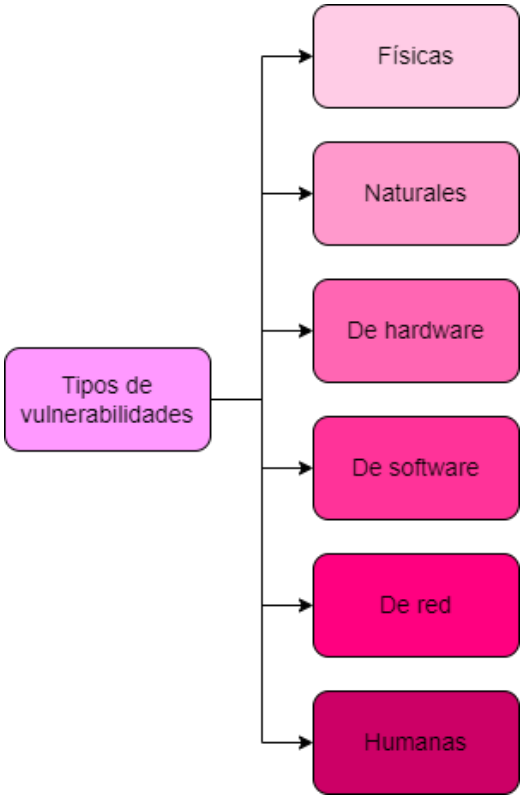


Figura 2.2. Tipos de vulnerabilidades

2.2.2.1 Físicas

Estas vulnerabilidades son las que se presentan en el entorno en el que la información se almacena, éstas hacen referencia a la posibilidad de que alguien no autorizado tenga acceso a los dispositivos físicos que albergan el sistema, si este tipo de vulnerabilidad es explotada afectaría directamente a la triada CID, en especial a la disponibilidad.

Una manera de proteger físicamente los equipos y evitar que esta vulnerabilidad sea explotada comienza desde mantener un acceso controlado a las instalaciones de la organización, y ya dentro de ella llevar a cabo la instalación de sensores biométricos que permitan solamente el acceso al personal autorizado, así como un método adicional de autenticación y la instalación de circuitos CCTV (Closed Circuit Television o Circuito Cerrado de Televisión).

Es muy importante que los equipos físicos cuenten con medidas de seguridad para acceder a ellos, como autenticación por usuario y contraseña, combinado con listas de control de acceso, para que cada usuario pueda acceder a las diferentes partes del sistema acorde con los privilegios que tenga. Cabe mencionar que esta es una de las propuestas que se pueden usar ya que puede haber otros métodos que la organización decida utilizar para preservar la seguridad física de los dispositivos, puesto que si un usuario mal intencionado tiene acceso a ellos podría simplemente robarlos, modificarlos o destruirlos.

Otra de las formas de proteger los dispositivos físicamente es mantener los cuartos de equipos o centros de datos a una temperatura óptima, esto de acuerdo a la ubicación de la empresa, para que estos puedan trabajar de manera adecuada y así evitar la pérdida de información por sobrecalentamiento.

Dentro del cuidado físico de los dispositivos se tiene que hablar del calentamiento global, este es un fenómeno que se origina por la absorción de la energía solar, por lo que la Tierra al calentarse comienza a desprender calor hacia la atmósfera, parte de este calor vuelve a emitirse hacia la superficie de la Tierra y así de manera sucesiva, lo que trae como consecuencia el efecto invernadero, este es un fenómeno natural y beneficioso para los seres que habitan en la Tierra, sin embargo, las acciones del hombre han provocado un desequilibrio, provocando así el calentamiento global.

Las tecnologías de la información y comunicación también impactan en el calentamiento global, ya que representan el 4% de las emisiones de gases de efecto invernadero, y se prevé que para el 2025 aumente al 8%, por lo que es importante que las organizaciones tomen medidas para ayudar a que esto no suceda.

La tecnología verde, también conocida como tecnología limpia o tecnología ambiental pretende fomentar una amistad entre la tecnología y el medio ambiente, esto puede conseguirse diseñando soluciones o dispositivos basados en la ecoeficiencia, es decir, que se garantice un buen funcionamiento reduciendo el impacto ambiental. Esto se logra de la siguiente manera:

- Desarrollo de dispositivos amigables con el medio ambiente, es decir, que se haga una reducción de los recursos naturales en la fabricación de dispositivos, hasta la correcta eliminación de residuos.
- Creación de soluciones que mediante el uso de tecnología verde se generen soluciones eficientes, así como un ahorro en el gasto energético.
- Que se lleve a cabo una correcta gestión de residuos sólidos, es decir, una eliminación correcta de residuos electrónicos, recolección de materiales reciclables o la reutilización de los residuos de producción, solo por mencionar algunos.

El que las organizaciones inviertan en tecnología verde es una buena solución para empezar a reducir el impacto medioambiental, además de eso, este tipo de tecnologías puede aportar beneficios a las organizaciones ya que tendrían una reducción de costos y una mayor eficiencia operativa, además, las organizaciones que hacen uso de tecnología verde tienen una mejor reputación.

Como seres humanos hay que estar conscientes de todas las consecuencias que trae consigo el calentamiento global, por lo que esto no se tiene que tomar a la ligera. Es importante hacer conciencia y aplicar medidas para reducir el impacto.

2.2.2.2 Naturales

Estas se relacionan con los desastres naturales que pueden poner en riesgo el sistema, como inundaciones, terremotos, tornados, huracanes, tormentas, entre otros. Cada organización debe tener en cuenta qué tipo de precauciones debe considerar y que sean acordes a su ubicación geográfica de la organización.

Para minimizar este tipo de vulnerabilidad se pueden adoptar diferentes medidas, por ejemplo, en caso de tener cortes de luz se puede hacer uso de fuentes de respaldo que proporcionen la energía necesaria al sistema, para evitar que los dispositivos se dañen si llegan apagarse de manera repentina, también se puede hacer uso de sensores de humedad y temperatura para monitorear que las instalaciones en donde se encuentran los sistemas de información estén en condiciones adecuadas para que funcionen de manera óptima. Entre otras medidas que se pueden considerar necesarias se encuentra la instalación de sistemas contra incendios, esto para evitar que alguna acción ocurrida en otro piso afecte de manera directa a alguno de los dispositivos, también la instalación de circuitos de videovigilancia, para monitorear continuamente las diferentes partes de la organización y poder atender a tiempo los percances.

2.2.2.3 Hardware

El hardware, al referirse a la parte física de los dispositivos podría considerarse un elemento libre de vulnerabilidades, sin embargo, en los últimos años han surgido vulnerabilidades y exploits que pueden poner en riesgo la seguridad del hardware. Este tipo de vulnerabilidades es muy difícil que sean detectadas por las soluciones actuales de seguridad, como los antivirus, además de que es muy probable que si un dispositivo o componente de hardware se infecta ya no puede ser reparado.

Las vulnerabilidades en el hardware pueden deberse a diferentes motivos, entre ellos:

- Defectos en su fabricación.
- Errores en la configuración de los equipos que permitan hacer modificaciones no autorizadas.
- Falta de actualizaciones.
- Mantenimiento inadecuado del sistema
- Equipos de mala calidad.

Para reducir la ocurrencia de vulnerabilidades provocadas por error humano es indispensable leer los manuales técnicos de los dispositivos, ya que en estos se especifica como debe ser armado el equipo correctamente, y también explican cómo es que debe ser llevado a cabo su mantenimiento.

2.2.2.4 Software

Estas se producen por aplicaciones mal configuradas o mal diseñadas que permitan el acceso no autorizado al sistema, también es probable que se deban a programas en los que un usuario malicioso haga mal uso de los recursos.

Dentro de las vulnerabilidades de software se encuentran las vulnerabilidades de medios de almacenaje y de comunicación, las cuales se explican a continuación:

- **Medios de almacenaje:** los medios de almacenaje son aquellos medios físicos o magnéticos que se usan para guardar información, entre los cuales se encuentran las bases de datos, servidores y discos duros.
  Si alguno de estos medios de almacenaje no es usado de manera adecuada su contenido se vuelve vulnerable, afectando a la triada CID.
- **Comunicación:** la información viaja a través de la red haciendo uso de medios guiados y no guiados, cuando la información viaja debe tenerse en cuenta que debe hacerlo de manera segura para que llegue correctamente a su destino, para ello se tiene que aplicar seguridad a los medios sobre los que transita, para así evitar que los datos sean interceptados y se afecte la integridad y confidencialidad de los mismos, también se tiene

que evitar que haya fallas en la comunicación que provoquen que la información deje de estar disponible para los usuarios autorizados.

2.2.2.5 Red

Este tipo de vulnerabilidades pueden presentarse por diferentes factores, los cuales van desde una mala instalación de la red, que el cableado estructurado este mal diseñado o no se hayan seguido los estándares correspondientes.

Asimismo, se pueden presentar vulnerabilidades si la red esta sobresaturada, lo que ocasionaría que se quedara bloqueada y por ende inservible, vulnerabilidad que un atacante podría aprovechar para irrumpir en la red y así obtener la información o datos que necesite.

Otra vulnerabilidad que podría presentarse es la intercepción de la información que se transmite desde o hacia la red, el atacante al interceptar los datos podría efectuar algún tipo de ataque y así explotar dicha vulnerabilidad.

2.2.2.6 Humanas

Este tipo de vulnerabilidades tiene relación con los daños que puede provocar una persona a un sistema de información, el cual puede ser de manera intencional o accidental.

Las razones principales que provocan este tipo de vulnerabilidades inician con la falta de medidas de seguridad acordes al sistema, es decir, entre más dependan los sistemas del ser humano pueden ser vulnerados más fácilmente, esto porque algún atacante puede amenazar al encargado de salvaguardar la integridad del sistema para que revele las credenciales de acceso, y esto no tiene que ver con la falta de conciencia, conocimiento o capacitación sobre la seguridad, ya que el atacante puede efectuar sus amenazas involucrando cosas de la vida personal de la víctima, por lo que este cedería la información que se le solicite, aun estando consiente de que no debería hacerlo, una solución para esto es automatizar los sistemas, para que estos dependan cada vez menos del ser humano, así si algún atacante intenta atacar un sistema automatizado le sería más complicado obtener información de acceso, ya que ninguno de los empleados tendría dicha información.

Otra razón por la que se generan este tipo de vulnerabilidades es debido a las debilidades humanas, las cuales pueden ir desde la falta de capacitación para la realización de las actividades, hasta la falta de concientización sobre la seguridad.

Es importante que los empleados y usuarios del sistema sean capacitados correctamente para que sean conscientes de la importancia que tiene mantener la seguridad del sistema, también es importante que sepan lo que puede pasar en caso de que esta sea violada, para que así traten de evitar cometer errores que pongan en peligro todo el sistema.

Identificar las vulnerabilidades es una manera útil de conocer que ataque podría llevarse a cabo junto con sus consecuencias, teniendo esto en cuenta se puede tener una respuesta rápida en caso de que alguna de las vulnerabilidades sea explotada, y que así la información o el sistema no se vea afectada por completo.

(Cano Rubio, 2018; Delgado Avenia, 2017; Limones, 2022; Ptolomeo UNAM, s. f.-b, s. f.-a; Romero Castro et al., 2018; Tarazona T, 1969)

Tema 3. Identificación de ataques y técnicas de intrusión

3.1. Ataques

3.1.1 Definición

Un ataque a la seguridad informática puede ser definido como una acción que explota una vulnerabilidad o debilidad encontrada en el software o hardware, con el fin de perjudicar un sistema, alterar su funcionamiento o robar información de las organizaciones.

Los ataques pueden ser ocasionados por diferentes grupos de actores, entre ellos:

- **Hackers:** en el caso de los black hat y grey hat atacan el sistema en busca de un beneficio que por lo general es económico. En el caso de los white hat realizan los ataques a los sistemas con previa autorización para descubrir las vulnerabilidades del sistema y poder corregirlas y prevenir daños mayores.
- **Grupos organizados:** en esta categoría se encuentran grupos que atacan los sistemas con diferentes fines, por ejemplo, los terroristas realizan los ataques con fines criminales, mientras que los activistas los realizan con fines ideológicos.
- **Empresas privadas:** realizan los ataques a otros sistemas con diversas intenciones, cómo, por ejemplo, el espionaje o el sabotaje.

Todas las organizaciones son propensas a sufrir un ataque en cualquier momento, esto trae consigo un efecto negativo, porque impacta en la estructura de la organización, muchas veces imposibilitando el funcionamiento del sistema, lo que trae como consecuencia repercusiones económicas, a su imagen, y también su prestigio, viéndose afectados entre otros los clientes y proveedores de la organización.

Cuando una organización es víctima de un ataque además de la pérdida de dinero, está la perdida de reputación, clientes, inversionistas, credibilidad, crecimiento, entre otras, lo que hace que cualquiera de ellas sea una buena razón para usar medidas preventivas con la finalidad de evitar ataques y fallas en la seguridad. Con el uso de mecanismos preventivos se puede disminuir el impacto de los ataques, sin embargo, hay una barrera muy grande al momento de que una empresa quiere aplicarlos, ya que se necesita aceptación y compromiso de los involucrados, para que comprendan su importancia como parte de un proceso que beneficia a la organización.

Un buen mecanismo preventivo es realizar una simulación de ataque, este permitirá identificar las vulnerabilidades del sistema, ver el daño que causan y como es que la organización se puede recuperar de una situación similar.

(Delgado Avenia, 2017; Hosting Perú, 2017; Mieres, 2009)

3.1.2 Ataques inherentes a las redes

En el tema 2, se mencionaron las fuentes de amenaza y los tipos de vulnerabilidades a los que se enfrenta un sistema, sin embargo, no se mencionaron la seguridad física y lógica, y éstas son muy importantes para proteger el sistema de una mejor manera.

3.1.2.1 Seguridad física

Es la que brinda protección al hardware y a las instalaciones físicas de toda organización, identificando y analizando las amenazas a las que se pueden enfrentar la infraestructura, los bienes o los procesos, con el fin de implementar medidas para prevenir la ocurrencia de acciones que puedan dañar el sistema de manera física.

A continuación, se mencionan algunas de las amenazas más frecuentes y los mecanismos a tener en cuenta para implementar adecuadamente la seguridad física:

- **Incendios:** para proteger los dispositivos contra una amenaza de este tipo se debe de considerar que estos deben estar alejados de zonas donde se manejen o almacenen sustancias altamente inflamables o explosivas, otra recomendación es que se debe de contar con sistemas antiincendios, detectores de humo o extintores para que en caso de ser necesario se pueda sofocar el incendio en el menor tiempo posible y así evitar grandes pérdidas.
- **Inundaciones:** para proteger los dispositivos de las inundaciones hay que evitar que los equipos físicamente se encuentren en plantas bajas o sótanos donde el riesgo de que entre agua superficial es mayor, asimismo se deben de contar con otras medidas que complementen la protección, como lo es contar con paredes y techos impermeables y sellar las puertas para evitar que entre el agua de pisos superiores.
- **Daño humano:** hay que tomar en cuenta que los desastres naturales no son los únicos que pueden afectar los dispositivos de hardware, ya que puede haber personas mal intencionadas que quieran afectar físicamente los equipos, y esto pueden hacerlo de diferentes maneras, una de ellas es que alguien no autorizado entre al cuarto donde se almacenan los dispositivos y directamente robe información almacenada en ellos o incluso robe físicamente parte del equipo, otra forma es dañando el cableado estructurado del sistema, por lo que hay que proteger el lugar de almacenamiento con sensores biométricos, cámaras de seguridad, entre otros, y así evitar que personal no autorizado entre y dañe los equipos de manera accidental o intencional.
- **Señales electromagnéticas:** hay que considerar que las señales electromagnéticas pueden afectar el funcionamiento de los dispositivos, o del cableado estructurado, por lo que es importante mantener alejado el equipo de lugares con grandes emisiones de señales de este tipo, y en caso de que esto no sea posible hay que proteger el equipo

de hardware implementando filtros especiales que inhiban la propagación de dichas señales hacia los dispositivos.

- **Apagones y sobrecargas eléctricas:** para evitar que el sistema se apague de forma repentina y se pierda información importante, una opción es colocar fuentes de alimentación externas que proporcionen electricidad durante un periodo de tiempo suficiente para que el sistema continúe trabajando, además, para proteger los dispositivos de hardware de sobrecargas eléctricas se deben de incorporar filtros que estabilicen la electricidad y evitar así picos de voltaje que puedan dañar el sistema.

(Iriarte Medina, 2006)

3.1.2.2 Seguridad lógica

Para complementar a la seguridad física se deben de implementar medidas de seguridad lógica que protejan el software almacenado en los equipos, esto con el fin de evitar pérdidas de datos, la entrada de algún malware, modificaciones no autorizadas, entre otras acciones que imposibiliten el acceso a los equipos.

La seguridad lógica consiste en aplicar procedimientos que garanticen que los datos almacenados solo podrán ser accedidos por usuarios, sistemas o procesos autorizados. A continuación, se mencionan algunas amenazas lógicas que se pueden presentar, así como mecanismos de defensa que se pueden implementar para mejorar la seguridad lógica:

- **Robos:** para evitar que la información o datos sean robados, es importante que ésta no sea almacenada en texto plano, porque esto facilitaría las cosas al atacante, cifrar la información es una buena opción para que en caso de que sea interceptada o robada no sea legible, además, el uso de contraseñas es importante para evitar que con solo tener acceso físico al dispositivo se tenga acceso a los datos que almacena.
- **Pérdida de información:** puede ser que por algún fallo del sistema o un error humano se pierda información importante, por lo que hacer copias de seguridad toma una gran relevancia para restaurar la información en caso de pérdidas, dichas copias se realizan en un sitio secundario, de donde los datos pueden ser rescatados cuando sea necesario, esto es, que los datos estén en un lugar lejano, al menos en otro edificio del lugar del cual se están protegiendo.

  Otra opción para minimizar los daños por pérdida de información es el uso de un grupo redundante de discos independientes mejor conocidos como RAID o Redundant Array of Independient Disks, este es un conjunto de discos independientes redundantes cuya finalidad es proteger los datos en caso de que algún disco duro falle. Un RAID consiste en crear un único volumen con varios discos duros funcionando en conjunto, con los cuales se consigue redundancia o tolerancia a fallos en dado caso que uno de los discos falle, además de proporcionar la recuperación de los datos en tiempo real.

- **Pérdida de la integridad en la información:** mantener la integridad de la información garantiza que los datos enviados y almacenados no sean alterados por usuarios, sistemas y procesos no autorizados, por lo que es importante cuidar este aspecto. Una forma de mantener la integridad de la información al ser enviada es hacer uso de las firmas digitales, este es un método bastante útil para saber si la información fue o no alterada en el trayecto a su destino.
- **Malware:** el malware abarca virus, gusanos, troyanos, spyware o ransomware, que afecte la red, estos pueden permanecer latentes por cortos o largos periodos de tiempo, por lo que es importante hacer uso de antimalware para evitar que los dispositivos sean infectados por programas mal intencionados que roben información o modifiquen el comportamiento del sistema. Hay software antimalware que además de detectar la presencia de malware hace un seguimiento constante de los archivos para detectar anomalías y reparar daños que se puedan presentar.
- **Seguridad en la red:** implementar seguridad en una red implica combinar capas de defensa donde se implementen políticas y procedimientos con el objetivo de que únicamente los usuarios con autorización tengan acceso a los recursos. Hay diferentes formas de implementar seguridad en una red entre las cuales se encuentran:
    - **Firewalls:** estos pueden instalarse en forma de software o de dispositivos de hardware que examinan la información que pasa por la red, ponen una barrera entre la red interna y las redes externas, y esto lo hacen configurando las políticas de seguridad informática de la organización mediante reglas que permiten o deniegan la entrada de tráfico.
    - **Segmentación de la red:** segmentar la red es un proceso donde la red se divide en redes más pequeñas (subredes), con el propósito de mejorar el rendimiento de la red y sobre todo ayuda a mejorar las condiciones de seguridad, ya que se puede clasificar el tráfico en distintas categorías, lo que hace que sea más fácil aplicar las políticas de seguridad.
    - **Sistemas de detección de intrusiones:** también llamados IDS cuyas siglas significan Intrusion Detection System, como su nombre lo indica, detectan accesos no autorizados a la red, es decir, monitorean el tráfico entrante y ante alguna actividad sospechosa emiten una alerta a los administradores del sistema para que tomen las medidas necesarias. Hay que hacer la aclaración de que un IDS solo detecta los accesos sospechosos y emite alertas de posibles intrusiones, pero no trata de mitigar dicha intrusión.
    - **Sistemas de prevención de intrusiones:** este tipo de sistemas también son conocidos como IPS o Intrusion Prevention System, estos analizan el tráfico de la red para prevenir al sistema de la ocurrencia de ataques e intrusiones. Estos sistemas analizan en tiempo real las conexiones, y mediante este análisis concluyen si se va a producir o si ya se está produciendo algún incidente de

seguridad. Un IPS además de lanzar alarmas puede descartar paquetes y anular conexiones si identifica un comportamiento sospechoso.

La seguridad en las redes es indispensable, esto se debe a que muchos de los ataques se hacen a través de ellas, por lo que se debe de invertir en su seguridad. Las organizaciones deben tener la capacidad de prevenir eventos negativos en la seguridad e invertir en la protección de las redes, dentro de esto se incluye la prevención de acceso no autorizado, la modificación de información, la descarga de información confidencial sin previa autorización, entre otros.

Para mantener la seguridad en la red se implementan diferentes capas de defensa, con las cuales los usuarios autorizados tienen acceso a los recursos mientras que los usuarios no autorizados son bloqueados para evitar que ataquen vulnerabilidades que amenacen la seguridad.

Un sistema informático se compone de cinco elementos:

- Hardware.
- Software.
- Datos.
- Memoria.
- Usuarios.

Cualquiera de estos elementos puede ser aprovechado por un atacante, por lo que deben considerarse por igual como elementos vulnerables a un ataque.

Los principales objetivos de ataque son: los datos, el hardware y el software, los cuales pueden verse como un flujo, por lo que los ataques se clasifican en cuatro tipos: interrupción, intercepción, modificación y fabricación.

- **Interrupción:** la finalidad de un ataque de interrupción es destruir algún recuso y que éste quede inutilizable o no disponible afectando directamente a la disponibilidad. Este ataque es detectado de manera inmediata tanto por el sistema como por los usuarios. Una forma de representarlo gráficamente es la que se muestra en la figura 3.1.

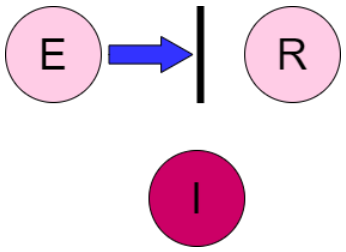


Figura 3.1. Ataque de interrupción.

(Iriarte Medina, 2006)

- **Intercepción:** este tipo de ataque se lleva a cabo cuando una entidad no autorizada accede a algún recurso, afectando directamente la confidencialidad. Este tipo de ataque es más complicado de detectar, debido a que no se producen alteraciones en el sistema. Su representación gráfica es la que se muestra en la figura 3.2.

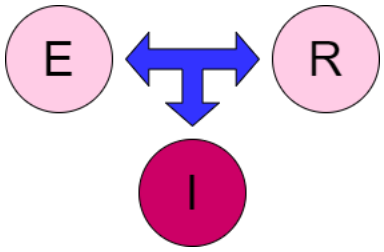


Figura 3.2. Ataque de intercepción.

(Iriarte Medina, 2006)

- **Modificación:** este tipo de ataque atenta contra la integridad, ya que la entidad no autorizada que accede al recurso en cuestión es capaz de manipularlo para su beneficio, este tipo de ataque suele ser muy dañino, ya que al manipular el recurso tiene la capacidad de dejar dispositivos inutilizables, o modificar los programas para que funcionen de forma distinta, además, dependiendo de las circunstancias un ataque de este tipo resulta difícil detectarlo. Gráficamente se puede observar en la figura 3.3.

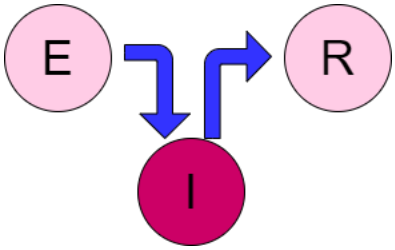


Figura 3.3. Ataque de modificación.

(Iriarte Medina, 2006)

- **Fabricación:** en este tipo de ataque, la entidad no autorizada que accede al recurso es capaz de insertar o crear objetos falsificados en el sistema, como direcciones IP, direcciones web o de correo electrónico, atentando directamente contra la autenticidad, detectar este tipo de ataque resulta bastante complicado. Gráficamente se observa en la figura 3.4.

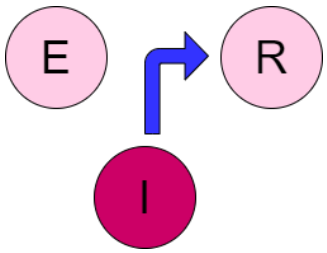


Figura 3.4. Ataque de fabricación.

(Iriarte Medina, 2006)

Identificar las vulnerabilidades presentes en todo sistema permite determinar qué tipo de ataques podrían efectuarse, teniendo esto en cuenta, la organización está en posibilidades de implementar medidas preventivas de acuerdo a las vulnerabilidades identificadas, incluso podría tener medidas correctivas en dado caso de que algún ataque se llevara a cabo.

(Cisco, s. f.-a; Iriarte Medina, 2006; López Barrientos & Quezada Reyes, 2019; Universidad Veracruzana, 2016)

3.1.3 Tipos de ataques

Cuando un sistema es atacado, lo que el atacante busca es conseguir privilegios en el sistema, de tal manera que esté en posibilidad de realizar modificaciones no autorizadas en su beneficio. Los tipos de ataques que pueden presentarse en un sistema se dividen en ataques pasivos y activos.

3.1.3.1 Ataques pasivos

Estos ataques solo observan el comportamiento o se leen y obtienen información sin alterar la infraestructura del sistema. Una particularidad importante de estos ataques es que monitorean el tráfico de la red, para llegar a la información confidencial que es la que al atacante le interesa, todo esto sin que los usuarios legítimos lo sepan, por lo que las organizaciones se deben de concentrar en prevenir este tipo de ataques, ya que la información obtenida puede ser usada durante un ataque activo.

El atacante puede obtener información usando alguno de los siguientes métodos:

- **Monitoreo de tráfico:** en una red se puede obtener el origen y el destinatario de la comunicación, esto se logra leyendo las cabeceras de los paquetes que circulan por dicha red.

- **Obtención de tráfico:** se puede obtener el control del volumen del tráfico intercambiado entre dos entidades que se comunican, con esto se obtiene información de la actividad en la comunicación.
- **Extracción de información:** para extraer información de los periodos de mayor actividad en el sistema, los atacantes pueden tener un control de las horas habituales en las que dos entidades hacen el intercambio de datos.

Los ataques de tipo pasivo suelen ser muy difíciles de detectar porque no provocan alteraciones en el sistema, sin embargo, la información recaudada en estos ataques puede ser usada en un ataque activo, por lo que es importante que la información que pasa por la red esté cifrada, esto para brindar una capa más de protección a la información y que el atacante no acceda a la información de manera directa.

3.1.3.2 Ataques activos

A diferencia de los ataques pasivos, los ataques activos sí afectan o modifican la información o estructura del sistema, asimismo, el flujo de datos transmitido puede sufrir modificaciones, entre los cuales se encuentra la creación de flujos de datos falsos, es decir, se ve involucrada la falsificación de los encabezados de los paquetes, para imitar a los usuarios legítimos y así acceder a los recursos.

Entre los principales objetivos de un ataque activo están: el sabotaje, robo de información o despliegue de malware, entre otros.

Los ataques activos suelen subdividirse en tres categorías:

- **Suplantación de identidad:** el atacante se hace pasar por una entidad distinta y de confianza para el sistema, esto con la finalidad de acceder a recursos privilegiados a los que normalmente no tendría acceso.
  Un ejemplo de esto sería cuando el atacante captura las secuencias de autenticación de su víctima para después repetirlas, con esto el atacante accede a los recursos suplantando así a una identidad legítima que sí posee los privilegios.
- **Modificación de mensajes:** este ataque se produce cuando el atacante altera un mensaje legítimo, con dicha modificación se producen actos no autorizados, por ejemplo, el mensaje legítimo es: “deposita mil dólares en la cuenta A”, el atacante al alterar el mensaje podría modificarlo a “deposita mil dólares en la cuenta X”.
- **Degradación fraudulenta:** estos ataques tienen como objetivo impedir el uso normal de los recursos, un ejemplo de esto sería que el atacante dificulte el envío de mensajes a una entidad en específico. Un ejemplo común de este tipo de ataque es la denegación de servicios, también llamado DoS del inglés Denial of Service.

La denegación de servicios tiene como objetivo inhabilitar el uso de un sistema, recurso o proceso, esto se logra mediante la generación masiva de peticiones al servidor desde un mismo equipo o dirección IP para consumir los recursos que ofrece el sistema hasta que este colapse y pierda su capacidad de respuesta por lo que comienza a rechazar las peticiones, materializando así la denegación de servicios.

Hay un ataque muy similar, llamado DDoS (Distributed Denial of Service) o denegación de servicios distribuidos, este ataque puede verse como la evolución del DoS, ya que se realizan múltiples peticiones al servidor al mismo tiempo, usando un gran número de dispositivos o direcciones IP. Para realizar este tipo de ataque, el atacante recluta dispositivos infectándolos con malware y así convertirlos en bots, los cuales son controlados de forma remota por el atacante. Un ataque de este estilo es más difícil de detectar, esto porque las peticiones provienen de diferentes direcciones IP y es muy complicado que el administrador del sistema sepa cuál es la dirección IP que realiza todas las peticiones.

Los ataques DoS y DDoS son usados para inhabilitar un servicio, ya que aprovechan las vulnerabilidades del sistema para hacer que este colapse, por lo que la disponibilidad se ve afectada de manera directa.

Los ataques que se realizan hoy en día han crecido de manera importante en número y en sofisticación, en términos generales todos ellos se pueden clasificar en tres categorías: phishing attacks, malware attacks y web attacks.

Phishing attacks

El phishing puede verse como un tipo de ingeniería social (tema 2.1) que los atacantes usan para conseguir información confidencial, como contraseñas o datos bancarios. En ese tipo de ataques, el perpetrador se hace pasar por alguien de confianza para que la víctima abra un mensaje de texto o correo electrónico mediante un enlace que direcciona al usuario hacia un sitio falso, una vez que el usuario accede a dicho enlace, el atacante puede ver información confidencial de su víctima o instalar un malware. Este tipo de ataques es una forma muy fácil de engañar a los usuarios y muchos de ellos caen por desconocimiento, temor e incluso curiosidad.

Los ataques que se realizan usando phishing pueden tener un amplio rango de objetivos, los cuales van a depender del atacante, incluso pueden ser dirigidos a alguna persona, una empresa o un gobierno en específico. A continuación, se explican algunas de las técnicas de phishing que los atacantes pueden llevar a cabo:

- **Spear phishing:** este tipo de ataques tiene como objetivo principal a una persona en específico de una organización, como puede ser el administrador del sistema, por ejemplo. Para realizar este ataque, el perpetrador recopila información de la víctima durante un periodo de tiempo, que pueden ser días, semanas e incluso meses, durante el cual investigan la mayor cantidad de información posible que les ayude a llevar a cabo

el ataque. Los perpetradores al momento de realizar el ataque, pueden incluir sitios web falsos o archivos infectados con malware, en dado caso de no ser así, los atacantes incluyen una secuencia de pasos que la víctima debe seguir para que el perpetrador logre su objetivo. Las víctimas suelen caer en este tipo de ataques porque al haber hecho una investigación previa de ellos sería complicado para la víctima distinguir el correo electrónico, archivo o enlace malicioso de uno legítimo.

- **Whaling phishing:** este ataque es mucho más dirigido que el spear phishing, ya que tiene como objetivo a personas con un perfil de directivo, como los CEO (Chief Executive Officer en español conocido como director ejecutivo) o CFO (Chief Financial Office, en español director financiero) ya que al tener puestos altos dentro de una organización tienen acceso a toda la información confidencial. Este tipo de ataque puede hacer que la víctima crea que quien lo contactó es una persona influyente o con un cargo de nivel superior dentro de la organización. Estos ataques actualmente están muy presentes y empresas como Mattel y Snapchat han sido víctimas de whaling phishing.
- **Smishing;** estos ataques se realizan mediante mensajes de texto o SMS (Short Message Service o Servicio de Mensajes Cortos), el atacante envía un mensaje a un teléfono móvil que contiene un enlace malicioso. Un ejemplo muy común de este tipo de ataque es cuando la víctima recibe un mensaje que parece provenir de una institución bancaria, informándole que su cuenta ha sido comprometida, el atacante haciéndose pasar por alguien de confianza le pide a la víctima que le ayude a verificar algunos datos, y una vez que los obtiene el atacante puede tomar el control de la cuenta bancaria de la víctima.
- **Vishing:** el atacante suplanta un número de teléfono para que parezca legítimo, por lo que realiza llamadas para hacerse pasar por un técnico, compañero de trabajo o alguien más que sea de confianza para la víctima, con la finalidad de obtener información confidencial. Algunos de los atacantes optan por usar filtros de voz en las llamadas para mantener oculta su identidad.

Malware attacks

Un malware es un software malicioso que invade, daña o deshabilita los sistemas, y asume el control de las operaciones. Un malware ocasiona daños de diferentes formas, ya que puede cifrar o borrar información, secuestrar funciones del sistema e incluso espiar la actividad del sistema sin que la víctima lo note.

Dentro de esta clasificación se encuentran muchos tipos de malware, por ejemplo:

- **Ransomware:** es un software que, al entrar en el sistema de la víctima, le da al atacante diferentes privilegios como bloquear el sistema desde un dispositivo de forma remota o cifrar archivos de la víctima, quitándole el control de toda la información que tiene almacenada, para después pedir un rescate a cambio de devolverle a la víctima los documentos que interceptó.

El ransomware se transmite como un troyano, es decir, infecta el sistema operativo ya sea con la descarga de archivos o explotando alguna de las vulnerabilidades del software.

- **Descargas automáticas:** es un método muy común para propagar el malware, para hacer esto, el atacante busca una página web insegura, en la que inserta un script malicioso en el código HTML o PHP, dicho script puede instalar el malware de forma directa en el dispositivo del usuario que acceda al sitio infectado, este tipo de ataque no requiere acciones de la víctima, solo es necesario que la víctima visite el sitio para llevar a cabo este ataque.
- **Troyano:** este es un software malicioso que intenta camuflarse como una herramienta útil, estos se propagan y persuaden a la víctima para que instale dicho software. Los troyanos son considerados un ataque muy peligroso e invasivo, además frecuentemente son diseñados para robo de información, y a diferencia de los gusanos, un troyano no tiene la capacidad de autorreplicarse, sin embargo, sí de robar todo aquello que tenga como propósito y su medio de propagación es muy diverso, ya que puede llegar mediante un correo electrónico, un sitio web que se haya visitado o incluso de un dispositivo USB de procedencia desconocida.

Web attacks

Este tipo de ataques tiene como objetivo aprovechar las vulnerabilidades de los sitios web para obtener acceso a información confidencial, introducir contenido malicioso o alterar el contenido del sitio. Dentro de este tipo de ataques se encuentran:

- **Inyección SQL:** es un método de infiltración que se beneficia de las vulnerabilidades en las aplicaciones, es decir, aprovecha los errores de diseño que hay en las páginas web. Las inyecciones de SQL son un problema grave de seguridad porque están relacionados con las bases de datos y se pueden emplear para manipular, robar o destruir datos.
  Los atacantes que realizan inyecciones de SQL engañan a las aplicaciones para lograr hacer uso de comandos que les permitan acceder a las bases de datos. Un ataque de este tipo puede ralentizar el funcionamiento de un sitio web, también puede ocasionar pérdida de datos o tomar el control absoluto del servidor.
- **Cross Site Scripring (XSS):** los ataques de este estilo hacen uso de recursos web de terceras personas para ejecutar secuencias de comandos en el navegador de la víctima. Estos ataques son una especie de inyección donde el atacante envía secuencias de comandos en forma de código JavaScript, los cuales son ejecutados por el navegador de la víctima. Este tipo de ataques suelen ser muy peligrosos y devastadores, sin embargo, actualmente muchos de los sitios cuentan con protección contra este tipo de ataques.

(Bello, 2023; García, 2023; IBM, s. f.; Kaspersky, 2023a; A. Moreno, 2021; Proofpoint, 2021; Romero Castro et al., 2018; Trend Micro, s. f.)

3.1.4 Etapas de un ataque

Si se conocen las diferentes etapas de un ataque se puede tener una perspectiva de la mentalidad del atacante, lo cual es útil para analizar la forma en la que el ataque se lleva a cabo, y así implementar las medidas de seguridad necesarias para garantizar una mayor seguridad dentro de la organización.

Tener conocimiento de las diferentes fases que forman un ataque es de suma importancia, ya que ayuda a las organizaciones a no subestimar la mentalidad del atacante al momento de llevar a cabo un ataque.

No hay un único modelo que explique las diferentes etapas de un ataque, por lo que en este apartado se mencionan tres modelos diferentes.

Primer modelo

En la figura 3.5 se muestran las diferentes etapas por las que pasa un ataque al ser ejecutado haciendo uso del primer modelo:

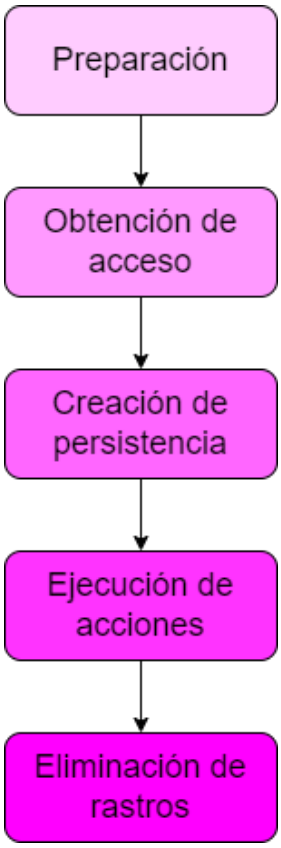


Figura 3.5. Primer modelo

Fase 1. Preparación

En esta primera fase, el atacante decide quién será su objetivo, posteriormente obtiene tanta información de la víctima como se necesite. Esta recolección de información puede ser activa o pasiva:

- **Pasiva:** se considera de este tipo cuando la recolección de información no puede ser detectada por la organización, algunos de los métodos para obtener información de forma pasiva son: buscar información de la organización y los empleados mediante algún motor de búsqueda, redes sociales, visitas a la página web de la organización, noticias, ingeniería social, entre otros.
- **Activa:** en este tipo de recolección el atacante deja rastros que pueden ser detectados por la organización, algunos de los métodos activos de obtención de información son: escaneos de red, análisis de activos expuestos en internet o discusiones en redes sociales, solo por mencionar algunos.

Lo siguiente que el atacante debe de hacer es crear o adquirir todas las herramientas con las que realizará el ataque, y esta fase concluye con la realización de pruebas para verificar que las herramientas con las que cuenta son capaces de evadir los controles de seguridad más comunes.

Fase 2. Obtención de acceso

Después de haber preparado el ataque, lo que sigue es obtener acceso al sistema víctima, para lograr esto se envían las herramientas recolectadas por diversos medios, como el correo electrónico (spear phishing o whaling phishing), sitios web infectados, dispositivos USB, entre otros.

Estas herramientas se envían con el objetivo de explotar las vulnerabilidades del sistema y evadir los filtros de seguridad para producir la intrusión inicial, al mismo tiempo, el atacante puede crear backdoors, para que pueda usar el sistema víctima en sus acciones futuras, y es en este momento cuando se crea el primer punto de presencia y control en el sistema víctima.

Fase 3. Creación de persistencia

Después de haber obtenido acceso se tiene que afirmar y ampliar la presencia y control del atacante sobre el sistema, para lograr esto tiene que empezar a moverse dentro del mismo, esto se conoce como *movimiento lateral.*

Uno de los principales objetivos de esta fase es conseguir los datos de autenticación que cuenten con el mayor nivel de privilegios, ya que estos le van a permitir al atacante realizar diferentes acciones para cumplir su objetivo. En esta fase es común que el código malicioso usado anteriormente sea actualizado, asimismo se generan nuevos payloads para disminuir la probabilidad de ser detectado.

Fase 4. Ejecución de acciones

A través del reconocimiento interno y de los movimientos laterales el atacante llega a los activos que son de su interés, y al contar con los privilegios de acceso que adquirió en etapas anteriores es capaz de recolectar la información y comenzar a realizar su extracción.

Fase 5. Eliminación de rastros

Después de que el atacante cumplió su objetivo, lo único que le queda por hacer es eliminar los rastros e indicadores que puedan revelar sus acciones, técnicas y procedimientos.

(Polanco, 2019)

Segundo modelo

El segundo modelo también consta de cinco fases, las cuales se muestran en la figura 3.6

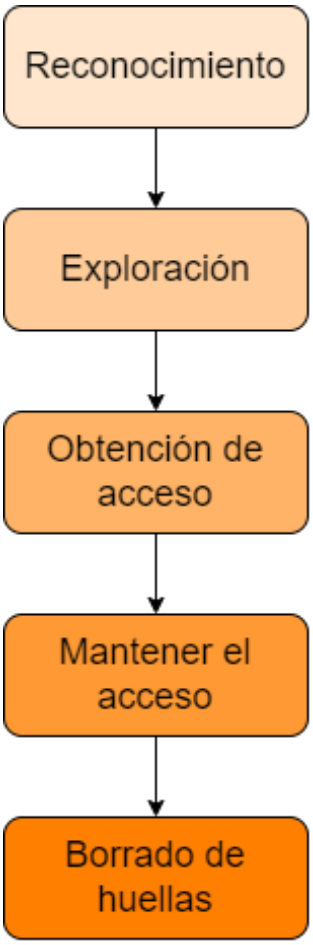


Figura 3.6. Segundo modelo

(Mieres, 2009)

Fase 1. Reconocimiento

Se recopila información de la víctima, ésta puede ser una persona, organización. Para obtener la información se hace uso de diferentes métodos, entre ellos se encuentra la ingeniería social o el monitoreo de la red.

Fase 2. Exploración

Se usa la información recopilada en la primera fase, con el objetivo de conseguir información del sistema víctima, como sus datos de autenticación, su dirección IP o su nombre de host, entre otros.

El atacante puede usar diferentes herramientas, entre ellas: mapeadores de red y puertos, escáneres de redes, puertos y vulnerabilidades.

Fase 3. Obtención de acceso

En esta fase es donde el ataque empieza a materializarse a través de la explotación de las vulnerabilidades encontradas en las primeras dos fases del ataque. Algunos de los métodos que puede usar el atacante en esta fase son: DoS, DDoS, secuestros de sesión, entre otros.

Fase 4. Mantener el acceso

Después de que el atacante consigue entrar en el sistema víctima, tendrá como objetivo implantar herramientas, esto con el objetivo de acceder más fácil en futuras ocasiones. Dentro de estas herramientas se encuentran las backdoors, rootkits y troyanos.

Fase 5. Borrado de huellas

Ya que el perpetrador accedió al sistema e instaló las herramientas de la fase anterior, hará el intento de eliminar los rastros que dejó en el proceso, con el objetivo de evitar que lo detecten. También intentará borrar archivos de registro y alarmas del los IDS

(Mieres, 2009)

Tercer modelo

El último modelo del que se hará mención describe siete fases que conforman un ataque y está dirigido a los administradores de seguridad, para que puedan identificarlo y detenerlo.

El modelo, también conocido como Cyber Security Kill Chain tiene origen en el sector militar, donde una *cadena de muerte* es un modelo que describe las etapas de un ataque y las formas de prevenirlo. Si el ataque es detectado al comienzo de la cadena se puede detener más fácilmente, porque entre menos información tenga el atacante es menos probable que pueda usarla en un ataque posterior.

Las capas de este modelo son las que se observan en la figura 3.7:

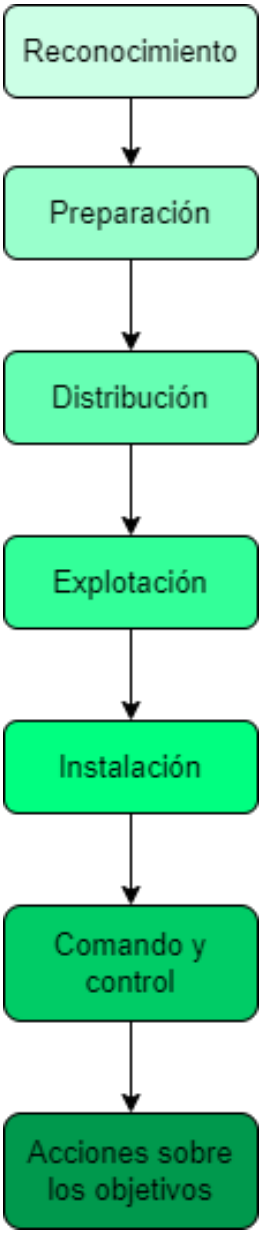


Figura 3.7 Tercer modelo

Fase 1. Reconocimiento.

Todo inicia con la recopilación de la información del objetivo a atacar, para hacer esto se hace uso de diferentes técnicas y herramientas como: motores de búsqueda, archivos web, servicios públicos en la nube, registro de nombres de dominio, analizadores de protocolos de paquetes, rastreo de red, escaneos de puertos, entre otros, con las cuales se pueden encontrar puertas de acceso a las aplicaciones, redes y bases de datos, por lo que es importante proteger la información para evitar que los atacantes localicen información comprometedora mientras navegan por los recursos que son públicos.

Fase 2. Preparación.

Después de tener la recopilación de la información, el atacante elige como va a iniciar el ataque al sistema, además toma en cuenta otros factores, como la capacidad de procesamiento o el tiempo estimado que le llevará realizar dicho ataque.

El ataque se puede iniciar abriéndose paso por la ruta que tenga menor resistencia, aun así, es importante para el atacante considerar todos los puntos de entrada existentes en el sistema, y para la organización es importante conocerlos para reforzar la seguridad, a continuación, se muestran algunos de estos puntos:

- Credenciales poco seguras o robadas.
- Servicios de acceso remoto, como SSH o VPN.
- Empleados poco capacitados en temas de seguridad.
- Cifrado deficiente o ausencia del mismo.
- Errores en la configuración del sistema.
- Phishing attacks.
- Web attacks
- Malware attacks.

Basta con que el atacante tenga éxito en un solo punto de ataque para entrar en el sistema, y una vez dentro lo siguiente que debe hacer es encontrar distintas formas de moverse libremente a través del sistema, para elevar sus privilegios de acceso y encontrar más fácilmente información de su interés, de igual manera debe intentar mantenerse oculto la mayor parte del tiempo. Por otro lado, los administradores o los encargados de la seguridad pueden adoptar principios de confianza cero, estos solicitan de manera constante la reafirmación de la identidad de los usuarios que se mueven dentro del sistema.

Fase 3. Distribución

Después de que el atacante entró con éxito a la red puede comenzar a distribuir la carga de malware, ransomware o lo que haya preparado para el ataque, también puede configurar programas para que el ataque se realice de manera inmediata o programada, incluso tiene la capacidad de hacer un ataque desencadenado o también llamado ataque de bomba lógica, donde los efectos planeados por el atacante se ejecuten después de que los usuarios víctimas realicen ciertas acciones.

Para prevenir la distribución de la carga maliciosa, los encargados de la seguridad deben realizar la inspección del tráfico en el sistema para detectar actividades inusuales.

Fase 4. Explotación

Después de que el atacante distribuyó la carga maliciosa es cuando comienza la explotación del sistema, la cual depende del tipo de ataque, que como ya se mencionó puede ser un ataque

programado, un ataque inmediato o una bomba lógica. La carga maliciosa regularmente debe tener características que oculten su actividad y origen para evitar ser detectados.

Después de que la carga maliciosa es activada, el atacante puede proceder a realizar el ataque según lo que tenga planeado.

Fase 5. Instalación

Si el atacante ve una oportunidad para realizar otro ataque en un futuro debe de instalar un backdoor para entrar y salir de la red sin que corra el riesgo de ser descubierto si vuelve a entrar por algún otro punto de falla.

Las backdoors se pueden instalar a través de rootkits y credenciales débiles siempre y cuando su instalación no presente señales que alerten a los encargados.

Fase 6. Comando y control

Después de que la carga maliciosa y las backdoors están instaladas, el atacante procede a tomar el control del sistema para ejecutar el ataque, las acciones que realice en esta etapa tienen como fin mantener el control de la situación, por lo que puede hacer la instalación de ransomware, spyware u otros medios que le ayuden al atacante a filtrar la información al exterior.

Es importante que los encargados de seguridad cuenten con medidas de protección que controlen y evalúen el sistema en busca de actividad sospechosa, ya que si el atacante comienza a extraer información será demasiado tarde, porque esto indica que el atacante ha tomado el control del sistema.

Fase 7. Acciones sobre los objetivos

Esta es la fase de ejecución, es aquí cuando el atacante emprende acciones maliciosas sobre el sistema víctima, dentro de las cuales se encuentran: el cifrado de datos, la denegación de servicios o la caída del sistema, solo por mencionar algunos.

Para evitar que el atacante llegue a esta fase, es importante el monitoreo continuo del sistema, para así detectar comportamientos sospechosos en tiempo real, y que los encargados de seguridad puedan detener el ataque a tiempo, es importante recordar que siempre es mejor prevenir los ataques en vez de detectarlos, ya que si se detectan demasiado tarde es perjudicial para la organización.

Después de haber conocido tres modelos diferentes que muestran las fases de un ataque, se puede observar que éstos tienen muchas etapas en común, todos coindicen en iniciar con la búsqueda de información de la víctima, para posteriormente usarla y encontrar información del sistema que se pretende atacar, también todos concuerdan en que si el atacante quiere mantener el acceso debe de instalar backdoors, para evitar ser detectado a la siguiente vez que quiera o necesite entrar al sistema, finalmente todos tienen en común que el atacante debe ser

sigiloso para evitar ser descubierto, y que también debe borrar el rastro que fue dejando previo a realizar el ataque para evitar ser descubierto.

(Netskope, s. f.)

El siguiente cuadro comparativo muestra un resumen de los métodos anteriores:

Tabla 3.1. Etapas de un ataque

Modelo 1	**Modelo 2**	**Modelo 3**
Se conforma de 5 etapas.	Se conforma de 5 etapas.	Se conforma de 7 etapas.
La recolección de información puede ser activa o pasiva. Se envían herramientas para explotar las vulnerabilidades del sistema y así acceder a él. Mediante el movimiento lateral se consiguen credenciales de acceso con el mayor nivel de privilegios posible. Con el movimiento lateral y el reconocimiento del sistema se encuentran la información de interés que se quiere extraer. Elimina los rastros que pudiera haber dejado, para evitar ser detectado.	Se recolecta información de la víctima, mediante ingeniería social, monitoreo de la red o cualquier otro método. Con lo anterior, se recolecta información del sistema que se quiere atacar. Se explotan las vulnerabilidades encontradas para acceder al sistema. Se implantan herramientas para que el atacante pueda acceder en un futuro si es necesario. Se eliminan los rastros que se pudieron haber dejado para evitar ser detectado.	Se recopila información del objetivo a atacar. El atacante analiza los puntos de falla descubiertos para entrar al sistema y moverse libremente dentro de él. Una vez dentro del sistema el atacante distribuye la carga con la que llevará a cabo el ataque. El perpetrador realiza el ataque de acuerdo con lo que tiene planeado. Se instalan backdoors para entrar en un futuro al sistema si es necesario. El atacante toma el control del sistema para ejecutar el ataque. Después de tomar el control del sistema el perpetrador realiza el ataque.
En los tres modelos se pueden observar ciertas similitudes, por ejemplo, todos inician con la recolección de información de la víctima, con dicha información el intruso accede al sistema para después llegar a la información que es de su interés, después, instala herramientas que le permitan acceder en un futuro y finaliza con el borrado de huellas para evitar ser descubierto.		

3.2. Reconocimiento y obtención de información

3.2.1. Bases de datos públicas

Una base de datos es una herramienta donde se recopila y organiza información, regularmente se almacena en un sistema informático y está controlada por un sistema de gestión de base de datos o Data Base Management System (DBMS), que en conjunto se denominan sistema de base de datos o simplemente base de datos.

En una base de datos puede almacenarse información sobre personas, productos, pedidos, entre otros, dicha información se encuentra ordenada de tal forma que es posible buscar los datos de manera rápida. Algo que cabe resaltar, es que una base de datos también necesita ser limpiada periódicamente ya que puede desordenarse o necesitar que se actualice la información que almacena.

Las vulnerabilidades en una base de datos se deben a que éstas se programan para dar dinamismo a las páginas, por lo que el programador de la base de datos no está tan consciente de que con un solo fallo de seguridad se puede poner en riesgo todo el sistema en dónde la base de datos está alojada. Entre las vulnerabilidades más comunes de las bases de datos se encuentran:

- **Nombre de usuario o contraseña en blanco o débil:** las contraseñas son la primera defensa de la información, por lo que se tiene que hacer uso de contraseñas que sean lo suficientemente seguras y que sean complicadas de conseguir por el atacante.
  Para crear contraseñas seguras es recomendable atender los siguientes pasos:
  - Hacer uso de letras mayúsculas, minúsculas, números y carácteres especiales.
  - Considerar la longitud de la contraseña, ya que ésta tiene un papel muy importante, y por ello es recomendable que tenga como mínimo ocho carácteres.
  - No hay que usar secuencias de caracteres (123 o abc) o secuencias como las que aparecen en el teclado (qwerty).

  Siguiendo estas recomendaciones es más seguro crear una contraseña que sea lo suficientemente fuerte para que ésta no pueda ser adivinada fácilmente.
- **Preferencia de privilegios de usuario por privilegios de grupo:** un error muy común es dar a los usuarios más privilegios de los que realmente necesitan, esto puede ocasionar muchos problemas, ya que de manera accidental o intencional pueden hacer modificaciones no autorizadas, por lo que es recomendable modificar el acceso de cada usuario de acuerdo a sus privilegios.
- **Desbordamiento de búfer:** éste es uno de los métodos más usados por los atacantes, se dan por enviar un exceso de información, es decir, se produce cuando se recibe más información de la que se espera. El desbordamiento de búfer trae diversas

consecuencias, entre ellas: la base de datos pierde estabilidad, puede bloquearse o devolver información corrupta, entre otras.

- **Datos sensibles sin cifrar:** cifrar la información que se almacena en la base de datos es una muy buena práctica, esto para que en caso de que un atacante logre hackear la base de datos le sea más complicado leer la información que se encuentra almacenada. Además de cifrar la información se pueden cifrar las contraseñas de acceso, esto puede hacerse usando algoritmos de cifrado, como MD5 (Message Digest Algorithm o algoritmo de resumen de mensajes).
- **Inyecciones SQL:** éste es un ataque, donde el intruso inserta su propio código en algún sitio de su interés, lo cual puede ser a través de un correo electrónico, una memoria USB o cualquier otro vector de ataque, con el fin de abrir una brecha en las medidas de seguridad para acceder a la información confidencial, después de que hace esto, toma el control de la base de datos, por lo que puede copiar, robar o modificar los datos almacenados.

Como se pudo observar, la seguridad de las bases de datos es muy importante por el tipo de información que albergan, por lo que hay una serie de recomendaciones para proteger las bases de datos de posibles vulnerabilidades:

- **Identificar su sensibilidad:** para proteger correctamente el sistema o la base de datos hay que conocer sus vulnerabilidades, así se pueden idear estrategias que ayuden a mejorar la seguridad del sistema.
- **Evaluación de vulnerabilidades y la configuración:** es importante evaluar las configuraciones de la base de datos para descartar los agujeros de seguridad, un ejemplo es la comprobación de los privilegios de los usuarios respecto a las acciones que tienen permitido ejecutar.
- **Monitorizar las acciones relacionadas con la base de datos:** es importante monitorear las actividades que realizan los usuarios, con esto los administradores se pueden dar cuenta si alguno de ellos está usando sus privilegios de forma indebida, esto también puede ayudar en la detección de intrusos.
- **Control de acceso y gestión de derechos:** es importante crear una jerarquía para garantizar que cada usuario solo pueda realizar las acciones que tiene permitidas, esto a su vez ayuda a garantizar la integridad de la información.

(Acens, s. f.; HN, 2020; Oracle, s. f.)

3.2.2. WEB

La World Wide Web, WWW, W3 o WEB es un sistema interconectado de páginas públicas mediante hipertexto, que son accesibles a través de internet.

El internet no es lo mismo que la web, este es una red global de servidores que hace posible el intercambio de información que ocurre a través de la web, mientras que la web es una aplicación construida sobre el internet, por lo que, para poder usar la web, es necesario tener acceso a internet y contar con un navegador web. El navegador web se comunica con el servidor web mediante el protocolo HTTP (Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertextos) para transmitir datos y compartir información.

Las páginas web son la unidad informativa de la web, son documentos compuestos de texto, imágenes, audios o animaciones que se crean usando HTML, el cual es un lenguaje de etiquetas de hipertexto que define el significado y la estructura del contenido web.

El hipertexto es un conjunto estructurado de imágenes, sonidos o textos interconectados mediante vínculos y conexiones lógicas, con éste se pueden realizar saltos dentro de la misma página o a otra página, así esté localizada en otro servidor. El hipertexto suele aparecer subrayado y en un color diferente, para resaltarlo del resto del texto.

Tim Berners Lee es considerado el padre de la WWW, diseñó el primer navegador de la historia llamado World Wide Web desarrollado con NEXTSTEP y también creó el primer servidor web, el cual se llamaba HTTPD (HyperText Transfer Protocol Daemon, que en español significa Demonio del Protocolo de Transferencia de Hipertexto).

La web tiene una arquitectura cliente – servidor, de tal forma que los servidores son los proveedores de información que atienden las peticiones de los programas cliente, es decir, de los navegadores, que son manejados por los usuarios finales.

La web al ser una red muy grande se ve constantemente amenazada de diversas maneras, una de ellas es ocultando código malicioso en las páginas web, muchas veces ese código es ejecutado por los usuarios de manera inconsciente, por lo que hay formas a través de las cuales un usuario puede verificar que está navegando por internet de manera segura:

- **Comprobar el nombre de la URL:** para asegurarse de que se está accediendo al sitio legítimo y no a un sitio falso creado por algún atacante.
- **Verificar los certificados SSL:** revisar si la página a la que se accede tiene el candadito en la barra de direcciones, lo que indica que es un sitio seguro, haciendo clic en el candadito se puede ver el certificado SSL y con ello saber si es una página oficial.
- **Evaluar la apariencia del sitio web:** al estar navegando en un sitio web el usuario podría notar indicadores que le alerten que es posible que se encuentre en un sitio falso, entre los cuales se encuentran:
    - Hay publicidad de productos que no son de interés para el usuario.

    - Los hipervínculos direccionan a sitios que al usuario no le interesa conocer.
    - Hay más ventanas emergentes de lo habitual.
- **Verificar la URL:** si la URL comienza con HTTP o HTTPS es un indicador de si el sitio está o no cifrado, si el sitio inicia con HTTPS indica que dicho sitio cuenta con un certificado SSL, por lo que se considera un sitio seguro, mientras que si empieza con HTTP significa que el sitio no cuenta con un certificado SSL, por lo que se considera un sitio poco confiable

La regulación de esta red es sumamente complicada, por lo que al usarla de manera constante los usuarios se exponen a los diferentes tipos de amenazas existentes.

(Foro Histórico de Telecomunicaciones, s. f.; MDN Web Docs, 2023)

3.2.3. DNS

En la década de los 70, en un archivo se tenían listados los nombres de los equipos conocidos y sus direcciones IP, este archivo llevaba por nombre “HOSTS.TXT” y se distribuía de manera periódica a los equipos conectados a la red, hasta ese momento no eran muchos, sin embargo, una década después, la cantidad de equipos conectados creció exponencialmente, por lo que distribuir la lista y evitar los nombres repetidos era una tarea sumamente complicada.

Paul Mockapetris, un científico informático estadounidense, reconoció el problema que había con el inicio del internet, notó la dificultad de mantener en el archivo HOSTS:TXT los nombres y direcciones de los dispositivos, por lo que propuso una base de datos distribuida cuyo contenido fuera esta información.

Es por esta razón que el 23 de junio de 1983 Paul Mockapetris y Jon Postel realizaron las primeras pruebas del Sistema de Nombres de Dominio o DNS que deriva del inglés Domain Name Server, el cual sentaría las bases para la popularización del internet.

El DNS son protocolos y servicios los cuales permiten usar los nombres de dominio en vez de las direcciones IP, es decir, le ayuda al ser humano a no memorizar direcciones IP, que pueden ser complejas de recordar, más en IPv6. El DNS traduce los nombres de dominio a su dirección IP, para que los navegadores puedan cargar los recursos de internet.

Todos los dispositivos conectados a internet tienen una dirección IP la cual puede verse como su identificador, con el cual otros dispositivos podrán encontrarlo. El funcionamiento de un DNS a grandes rasgos es el siguiente: el usuario escribe en el navegador web de su dispositivo la página que quiere visitar y el DNS se encarga de traducir el nombre de la página a una dirección que el dispositivo pueda entender, para que así pueda localizar la página web que el usuario necesita.

Los servidores DNS involucrados en la carga de un sitio web son:

- **Servidor raíz:** este se encuentra en la parte más alta de la jerarquía de servidores DNS, y es el encargado de traducir o solucionar los nombres de dominio a su dirección IP correspondiente.
- **Servidor de dominio de nivel superior:** estos servidores representan el siguiente nivel en la búsqueda de la dirección IP que se necesita, representan la extensión del sitio web. Se dividen en dos tipos:
    - **Dominios de Nivel Superior de Código de País (ccTLDs):** su longitud es de dos letras y corresponden a un país en concreto, es decir, representan un código de país o territorio, por ejemplo: .co, .au, .mx.
    - **Dominios de Nivel Superior Genéricos (gTLD):** su longitud es de tres letras o más, por ejemplo: .org o .net, estos son usados de manera genérica en todos los países, dependiendo de la organización.
- **Servidores de dominio de segundo nivel:** también son conocidos como SLD, son el nombre del sitio web sin contar la extensión, es decir, en: www.empresa.com, el dominio de segundo nivel es “empresa”. También se encuentran los ccSLD, estos representan a los dominios de segundo nivel de código de país, por ejemplo, en: www.empresa.com.mx el nombre de dominio de segundo nivel es “empresa.com”.
- **Servidores de dominio de tercer nivel:** estos hacen referencia a lo que se encuentra a la izquierda de los dominios de segundo nivel, no siempre están presentes en todos los sitios web, y puede verse como una representación para crear subdominios dentro de un sitio, son apartados específicos que permiten a los visitantes entrar de forma más directa a un contenido determinado.
- **Servidor de nombres recursivo:** este es un servidor que recibe las consultas desde los dispositivos de los usuarios, esto regularmente se hace mediante aplicaciones como navegadores web. Por lo general, este servidor es el responsable de mandar las solicitudes adicionales para satisfacer la consulta de DNS del cliente, en otras palabras, es el servidor encargado de realizar consultas a otros servidores a nombre del cliente.
- **Servidor de nombres autoritativo:** contiene la información sobre el nombre de dominio al que se quiere acceder, si cuenta con el acceso al dominio solicitado va a devolver la dirección IP al servidor de nombres recursivo.

La jerarquía del DNS tiene forma de árbol, iniciando en la parte superior con la raíz, esta se subdivide en ramas, las cuales representan a los servidores de dominio de nivel superior. El siguiente nivel son los servidores de dominio de segundo nivel, en estos se pueden encontrar registros del servidor de dominio de nivel superior asociado y debajo de este nivel se encuentran los servidores de dominio de tercer nivel (véase figura 3.8).

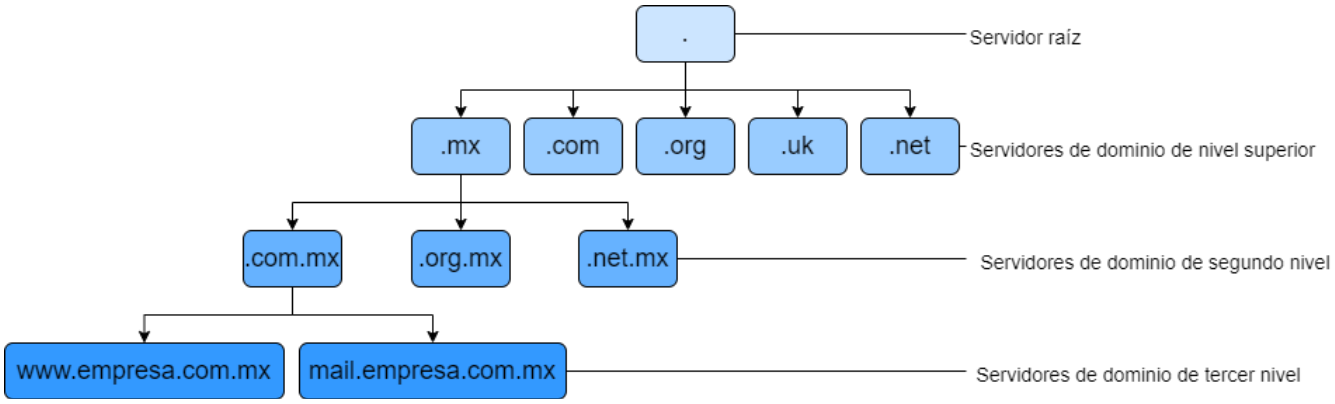


Figura 3.8. Jerarquía DNS.

Hay ocho pasos que explican el funcionamiento del DNS:

1. El usuario escribe en el navegador la página que quiere visitar, por ejemplo www.empresa.com, primero el navegador revisará si la información solicitada se encuentra en la caché DNS del dispositivo que realizó la petición, si ésta no se encuentra ahí se tiene que enviar la petición al servidor DNS recursivo, el cual generalmente es administrado por el proveedor de servicios de internet del usuario o ISP.
2. El servidor recursivo envía dicha solicitud al servidor raíz.
3. El servidor raíz le responde al servidor recursivo con la dirección IP del servidor de primer nivel que almacena la información del dominio solicitado, que en este caso sería ".com".
4. El servidor recursivo envía una solicitud al servidor ".com" de primer nivel.
5. El servidor de primer nivel le responde al servidor recursivo con la dirección IP del servidor de nombres de dominio de segundo nivel correspondiente, que de acuerdo al ejemplo es empresa.com.
6. El servidor recursivo obtiene la dirección IP que el usuario necesita y la envía al navegador web del usuario, al mismo tiempo, la almacena en la caché DNS del dispositivo, esto para responder con mayor rapidez la siguiente vez que esa solicitud sea enviada.
   Después de hacer la búsqueda del DNS y que se ha devuelto la dirección IP, el navegador puede hacer la solicitud para el sitio web.
7. El navegador envía una solicitud a la dirección IP que obtuvo del servidor recursivo, es aquí donde se encuentra el contenido que el usuario necesita.
8. Finalmente, el servidor de esa dirección IP devuelve la página web para que sea procesada por el navegador y que éste se la muestre al usuario.

Ataques a DNS

Como se puede observar, el DNS tiene un papel muy importante durante la navegación por internet y no está exento de ataques, estos buscan detectar vulnerabilidades en el protocolo,

con la finalidad de desviar al usuario y mandarlo a una dirección IP equivocada, esto puede tener muchos fines, como promover publicidad, hacer fraudes, distribuir spyware, entre otros.

Algunos de los ataques que se pueden hacer son:

- **Envenenamiento de caché:** es un método de ataque muy usado en el que el atacante busca redirigir el tráfico a páginas fraudulentas. Al acceder a una página que ha sufrido un envenenamiento de caché el atacante puede redirigir todo el tráfico a sitios que parecen ser legítimos, pueden hacer esto para robar datos de los usuarios.
- **Ataque DDoS contra servidores DNS:** esta práctica consiste en inundar con solicitudes los servidores usando botnets, esto ocasiona que los usuarios no puedan acceder con normalidad al sitio atacado, esto porque todas las solicitudes bloquean el servicio, lo que le genera grandes pérdidas económicas a la organización, ya que el sitio quedaría inhabilitado durante un tiempo indeterminado.
- **DNS spoofing:** este ataque busca afectar la experiencia del usuario, especialmente al ocurrir una suplantación en los datos de dirección del servidor DNS, lo que entorpece la navegación del usuario, ya que la navegación se ralentiza, o no abren los sitios web solicitados o se desvían a otros sitios.
- **DNS hijacking:** este tipo de ataque busca alterar la identidad del DNS establecida por el ISP, por lo que los nombres de los dominios quedan alterados y los usuarios acceden a servidores manejados por atacantes. En este tipo de ataque es muy común encontrar la existencia de sitios fraudulentos haciéndose pasar por sitios legítimos de instituciones bancarias o financieras, este es uno de los casos más comunes de fraude informático.

Después de conocer algunas de las amenazas que hay sobre los servidores DNS es importante tomar medidas de seguridad que ayuden a proteger los sistemas:

- **Mantener los sistemas actualizados:** se deben de mantener los sistemas actualizados, ya que hay muchas vulnerabilidades que pueden surgir y los atacantes pueden aprovecharse de ellas, por lo que todos los dispositivos deben de contar con las actualizaciones y parches de seguridad, para evitar que un atacante se aproveche de ello.
- **Herramientas de seguridad:** hay que mantener los sistemas protegidos, esto puede hacerse usando un antivirus el cual siempre debe estar actualizado, y es importante usar un firewall también, ya que éste ayudará a rechazar las conexiones fraudulentas que tengan como objetivo alguno de los dispositivos del sistema.
- **Usar conexiones seguras:** al navegar por internet es importante hacerlo mediante conexiones seguras, es decir, hay que evitar conectarse a través de redes wi-fi públicas ya que ponen en riesgo la privacidad de los usuarios, también es recomendable el uso de VPN’s especialmente cuando se haga uso de alguna conexión insegura, ya que estas ayudan a mantener la privacidad de los usuarios.

(Access Quality, 2023; AWS, s. f.; Cloudflare, s. f.; IBM, 2014; J. Jiménez, 2021b; NIC Argentina, 2018; Universidad de Jaén, s. f.; USS, 2019)

3.2.4. Keyloggers

Un keylogger es un software o dispositivo de hardware que registra en secreto las pulsaciones que un usuario hace en un teclado, la información obtenida es guardada en un archivo o en la memoria del dispositivo para que después sea enviada al atacante, donde puede leer toda la información que el usuario escriba, desde contraseñas, direcciones de correo electrónico, páginas web, entre otros.

Los keyloggers no fueron creados con la finalidad de robar información confidencial, se crearon como un medio de supervisión, por lo que son legales, sin embargo, su ilegalidad llega cuando son usados para espiar la actividad de los usuarios y robar información, cuando esto pasa son clasificados como spyware, esto porque capturan información confidencial para después enviarla a los atacantes y que éstos puedan explotarlo con fines delictivos.

No estar consciente de que todo lo que se escribe en el dispositivo está siendo monitoreado es un riesgo enorme, ya que el usuario víctima podría revelar al atacante información privada, tales como contraseñas, números de tarjeta, cuentas bancarias, entre otros, sin embargo, éstos han evolucionado, por lo que algunos tienen la capacidad de controlar la cámara, realizar capturas de pantalla, incluso robar información del portapapeles, algunos incluso pueden grabar las llamadas de voz o controlar el micrófono del dispositivo.

Tipos de keyloggers

Hay dos tipos de keyloggers, uno en forma de software y otro en forma de hardware:

- **Software:** es un programa que se instala en el dispositivo de la víctima, las formas más comunes de instalarlo son: a través del phishing, la ingeniería social, la descarga de archivos de sitios inseguros e incluso al abrir un archivo adjunto recibido por correo electrónico, después de que el keylogger se instala se ejecuta en segundo plano, comenzando a registrar las pulsaciones.
  Es muy complicado detectar este tipo de malware, ya que no siempre provocan problemas perceptibles en el dispositivo de la víctima, sin embargo, hay ciertas señales que pueden indicar que algo no anda bien en el dispositivo, como:
  - La navegación web es más lenta de lo normal.
  - Las pulsaciones se retrasan respecto a cuando se teclearon.
  - Aparición de ventanas de error al cargar gráficos o sitios web.

  Los keyloggers de software se dividen en:
  - **Keyloggers de kernel:** residen en el kernel del dispositivo, por lo que su detección es más difícil.

- **Keyloggers de API:** son los que usan las API de Windows (Application Programming Interfaces, en español conocidas como Interfaces de Programación de Aplicaciones) mediante las cuales se registran las actividades realizadas con el teclado.
- **Keyloggers de JavaScript:** estos keyloggers insertan código JavaScript en un sitio web, esto puede hacerse a través del ataque Cross Site Scripting.
- **Keyloggers de inyección de memoria:** este tipo de keyloggers se encarga de hacer modificaciones a las tablas de memoria que tienen un vínculo con las llamadas a las funciones del sistema, con estas modificaciones el keylogger puede evadir el control de las cuentas de usuario de Windows.

- **Hardware:** los keyloggers de hardware son independientes de los softwares instalados en el sistema operativo, ya que son dispositivos de hardware instalados en el dispositivo víctima. Este tipo de keyloggers se divide en:
  - **Keylogger firmware:** la BIOS (Basic Input - Output System o Sistema Básico de Entrada – Salida por su traducción al español) del dispositivo víctima se modifica para que registre los eventos al mismo tiempo que los procesa, en este caso, el software que se cargará en la BIOS debe ser elaborado especialmente para el hardware en el que se va a ejecutar.
  - **Keyboard hardware:** son dispositivos que se conectan entre el teclado y algún puerto de entrada del dispositivo de la víctima, con el objetivo de capturar todos los eventos realizados por el teclado.
  - **Wireless keyboard sniffers:** estos obtienen y almacenan los paquetes que se envían entre el teclado y el receptor.
  - **Keyloggers overlay:** se instala un teclado falso sobre el teclado auténtico, para que cuando el usuario presione una tecla, esta pulsación sea capturada por ambos teclados.

Detección y eliminación de keyloggers

Descubrir un keylogger a nivel de software puede ser sumamente complicado, ya que estos están diseñados para permanecer ocultos y porque cuando se ejecutan suelen hacerse pasar por un programa legítimo, sin embargo, hay formas de averiguar si hay o no keyloggers instalados, entre ellas:

- Se pueden buscar keyloggers en los procesos de ejecución, para esto se tiene que revisar el administrador de tareas y buscar algo que se esté ejecutando y no resulte familiar, sin embargo, solo expertos podrían reconocer este tipo de software.
- Otra opción es consultar el registro de la actividad del firewall para detectar si hay actividad sospechosa, es importante usar un firewall para comprobar todo lo que entra y sale del dispositivo, un keylogger envía los datos obtenidos a una ubicación remota, pero

para hacer esto necesita conexión a internet, por lo que quedará un registro de esto en la actividad del firewall.

- La forma más rápida de detectar y eliminarlos es usar un antivirus o una aplicación confiable para la detección de keyloggers.

Para detectar los keyloggers de hardware se tiene que revisar el dispositivo, ya que estos suelen ser pequeños dispositivos que se encuentran conectados entre el teclado y el equipo, tienen forma de adaptador y parece que forman parte de la configuración habitual de hardware por lo que sería difícil detectarlos si no se sabe cómo son. (Véase figura 3.9)

Figura 3.9. Keylogger de hardware.

[Fotografía]. (s.f.). Keelog. https://www.keelog.com/es/usb-keylogger/

Recomendaciones de seguridad

Para protegerse contra este tipo de amenazas se pueden seguir las siguientes recomendaciones:

- Usar un buen antivirus o detector de keyloggers y mantenerlo actualizado, además de contar con un firewall configurado correctamente de tal forma que se pueda bloquear el acceso a internet de algunas aplicaciones
- Mantener actualizado el sistema operativo, productos de software y navegadores, para contar con los parches de seguridad, evitando así que los atacantes saquen provecho de las vulnerabilidades.
- Usar gestores de contraseñas confiables, para evitar escribir las contraseñas en los sitios web a los que se quiera ingresar.
- Descargar software oficial, para evitar que se instale algún malware que venga oculto si se descargan los programas de fuentes no confiables.
- Bloquear el dispositivo cada que no esté en uso, con el fin evitar que alguien instale un keylogger directamente en el equipo.

(Kaspersky, 2023b; Latto, 2016; Mateiu, 2018; Tavella, 2021)

3.2.5. Ingeniería social

El término *ingeniería social* tiene origen en las ciencias sociales, hace referencia a cualquier esfuerzo de los factores de cambio para moldear el comportamiento de un sector de la población, de manera muy general, usa la manipulación para llegar a un fin.

La ingeniería social pueden verse como técnicas de manipulación psicológica y habilidades sociales que usan los atacantes para engañar a los usuarios y conseguir información confidencial, acceso a algún sistema, e incluso llevar a cabo actividades más elaboradas, como el robo físico de dispositivos, solo por mencionar algunas.

Para realizar ingeniería social, los atacantes van con sus víctimas haciéndose pasar por alguien de confianza que les puede ayudar a resolver el problema al que se enfrentan, el cual puede ser provocado por el mismo atacante, de esta forma se puede aprovechar de la falta de conocimiento de la víctima para la obtención de información, así como de la confianza que le tiene.

Lo más peligroso de la ingeniería social es que las víctimas no se dan cuenta que están siendo manipuladas hasta que notan las consecuencias, por lo que, para ese momento, el atacante ya ha logrado obtener la información confidencial que buscaba.

Tipos de ingeniería social

Debido a que la ingeniería social está basada en las reacciones humanas, hay diferentes formas en las que los atacantes pueden engañar a sus víctimas, el phishing (tema 3.1.3) es una de ellas, además hay otras técnicas, entre las cuales se encuentran:

- **Baiting:** el atacante puede dejar un dispositivo de almacenamiento en un espacio público como una USB infectada con algún software malicioso, el ser humano es curioso por naturaleza, por lo que alguien podría tomar dicha memoria e introducirla a su computadora para revisar su contenido, al hacer esto, el software malicioso de la USB se introduciría al equipo de la víctima.
- **Quid pro quo:** hace referencia a cuando los atacantes engañan a sus víctimas haciéndoles creer que se han ganado algún descuento o producto, diciéndoles que deben llenar algún formulario antes, en dicho formulario piden una gran cantidad de datos personales, los cuales el atacante usa para robar su identidad.
- **Farming:** al usar esta técnica, el atacante realiza una investigación previa de su objetivo, para después establecer una relación con su víctima, engañándola durante el tiempo necesario para obtener todos los datos que le interesan.
- **Spamming de contactos:** el atacante obtiene el usuario y contraseña del correo electrónico de su víctima, para después enviar correos de spam a todos sus contactos, quienes al recibirlos creen que quien lo envió es el usuario legítimo del correo por lo que al ser una persona de confianza proceden a abrir o descargar los archivos que les han

sido enviados, al hacer esto, el atacante tiene como objetivo difundir software malicioso o engañar a las demás víctimas para obtener información confidencial.

- **Tailgating:** se refiere a cuando el atacante entra sin autorización a un área reservada, esto lo consigue siguiendo a una persona autorizada e infiltrándose sin ser descubierto.
- **Piggybacking:** el atacante consigue entrar a la zona reservada, pero con previa autorización, la cual consigue engañando a personas autorizadas para que le permitan el acceso a las áreas restringidas que sean de su interés.

Métodos de protección

Protegerse de la ingeniería social comienza con la concientización, ya que todas las personas pueden ser víctimas de este tipo de ataque en algún momento, por lo que es recomendable seguir una serie de medidas preventivas, entre las cuales se encuentran:

- Comprobar las direcciones de los correos electrónicos recibidos, especialmente cuando se trata de proporcionar información confidencial, así mismo los usuarios deben de estar conscientes de no dar clic a enlaces o archivos adjuntos a menos que se esté completamente seguro de que su procedencia es confiable.
- No hay que divulgar información sensible con desconocidos o almacenarla en lugares públicos, donde los atacantes puedan acceder a los datos tan fácilmente.
- Dentro de las organizaciones se deben de implementar correctamente políticas de seguridad que ayuden a minimizar los riesgos, así mismo se debe de instruir a los empleados para que las lleven a cabo correctamente, explicándoles las consecuencias que puedan ocurrir. Un ejemplo de este tipo de políticas es tener bajo vigilancia las áreas restringidas, donde todas las personas que quieran acceder lo hagan a través de un sistema automatizado mediante una tarjeta con código de barras o un sistema biométrico y llevar un control de las mismas.
- Hay que instalar antivirus o software de protección como un firewall y mantenerlo actualizado para detectar las amenazas e impedir que se ejecuten.
- No hay que descargar software o archivos de fuentes desconocidas o poco confiables, mejor hay que hacerlo desde los sitios oficiales. También hay que evitar acceder a sitios no seguros para minimizar el robo de información.

La ingeniería social es un método muy usado en la obtención de información, por lo que hay que mantenerse alerta a cualquier señal que indique que algo anda mal, así como usar el sentido común ante cualquier situación que genere desconfianza.

(Argentina.gob.ar, 2020; Bodnar, 2020; INCIBE, 2019b; Kaspersky, 2024; Norton, 2018a; Sandoval Castellanos, s. f.; VIEWNEXT, 2020)

3.2.6. Dumpster diving

El dumpster diving o “recolección de basura”, es un método de obtención de información que consiste en buscar información en la “basura” de una organización, basándose en el dicho “la basura de un hombre es el tesoro de otro”, lo que quiere decir que lo que para algunas personas ya no es útil para otras sí, por lo que pueden sacarle provecho.

El dumpster diving hace referencia a la exploración en lo que se considera basura del sistema para obtener información que le permita llevar a cabo un ataque, por lo general, los atacantes buscan información confidencial en dicha basura por lo que cuando la organización elimine información debe hacerlo adecuadamente.

Entre la información que el atacante busca se encuentra:

- Credenciales de acceso, números telefónicos, correos electrónicos, domicilios de clientes, socios y proveedores, números de tarjetas de crédito y cuentas bancarias, entre otros.
- Diseños de productos, planos o borradores, así como secretos comerciales y de marketing.
- Dispositivos electrónicos y de almacenamiento portátil, como CDs, DVDs, USB y discos duros.
- Información del software usado por la organización víctima, así como de las herramientas y tecnologías que utilizan.

Para prevenir que los atacantes obtengan información usando este método hay que implementar medidas de seguridad, como la creación de políticas de retención de datos en las cuales se establece el tiempo que se deben de conservar los datos y como es que deben de ser desechados, adicionalmente se debe de crear un certificado de destrucción de datos sensibles. La destrucción de este tipo de datos se puede hacer con procedimientos manuales de bajo costo y uso de software especial, o también destruyendo físicamente los dispositivos que almacenan información.

Es importante mencionar que formatear los dispositivos electrónicos antes de desecharlos no borra los datos por completo, por lo que una buena opción es usar herramientas freeware, shareware o software comercial que eliminen eficazmente la información de los medios de almacenamiento.

Otra medida de prevención es crear conciencia en todas las personas que colaboran en la organización y proporcionar capacitaciones de borrado seguro, para que lleven a cabo correctamente las políticas implementadas a fin de crear hábitos que repliquen en todos los dispositivos a los que tengan acceso. Cabe mencionar que si bien no es recomendable permitir que los empleados lleven documentos impresos o equipos de trabajo a sus hogares por el riesgo

que representa, si esto llega a suceder se tiene la confianza de que seguirán correctas normas de seguridad.

(Borreda, 2021; Ciberseguridad, s. f.-b; Wright, s. f.)

3.2.7. Sniffing

Un sniffer es una herramienta que puede ser de software o hardware que permite monitorear y capturar el tráfico de una red en tiempo real. Los administradores de las redes suelen usar este tipo de herramientas para llevar un control del tráfico que circula por la red.

Los sniffers capturan los paquetes de datos que viajan por la red, por lo que los atacantes pueden usarlos para interceptar el tráfico de la red objetivo, con lo cual pueden obtener información confidencial de su interés.

Esta práctica, los atacantes pueden acompañarla de ingeniería social, para conseguir que las víctimas descarguen sus sniffers, esto puede hacerse dirigiendo a las víctimas a sitios infectados para que al hacer una descarga vaya integrado el sniffer de manera automática o por medio de archivos adjuntos enviados por correo electrónico. También hay sniffers de hardware, estos permiten revisar un segmento de la red en específico y al estar conectados directamente a la red se puede garantizar que no se perderán paquetes, un sniffer de hardware almacena los paquetes recolectados y los envía a un colector de paquetes que registra toda la información obtenida, para posteriormente analizarla.

Hay dos tipos de sniffing, el sniffing pasivo y el sniffing activo:

- **Sniffing pasivo:** en una red se pueden usar hubs, estos conectan varios dispositivos en la red, sin aplicar algún mecanismo de regulación que dirija el tráfico solo a su destino, por lo que todos los dispositivos de la red reciben todo el tráfico y después determinan si es relevante para ellos o no, teniendo esto en cuenta, se puede notar que el sniffer puede interceptar todo el tráfico de la red sin problema, por lo que solo hay que analizar los paquetes que circulan para determinar cuáles son los de interés, es justamente esta característica lo que hace que un sniffer pasivo sea difícil de detectar.
- **Sniffing activo:** en redes grandes se suelen usar switches, los cuales ayudan a regular el tráfico que viaja por la red, enviando los paquetes que reciben a su respectivo destino, de manera que para los atacantes es más conveniente usar un sniffer activo en este tipo de redes para así evadir las restricciones que crean los switches, una manera de hacer esto es inyectando tráfico adicional en la red, lo que hace que el sniffer sea más fácil de detectar.

Métodos de protección

El cifrado de los datos es una buena opción para proteger el tráfico del sniffing, esto para que en caso de que haya paquetes de datos capturados, los atacantes no puedan hacer uso de esta información a menos que logren descifrarla, también puede navegarse por la red usando una VPN, así toda la información viaja por la red en un túnel cifrado, por lo que viaja de forma segura.

Otra medida de protección es evitar conectarse a redes Wi-Fi públicas sin el uso de una VPN, ya que al ser una red pública cualquier persona que se conecte a dicha red puede ver los datos que circulan por ella.

Se debe de tener instalado un buen antivirus que sea capaz de detectar el malware que se pueda infiltrar en el sistema, asimismo, hay antivirus que son capaces de detectar sniffers y que ofrecen eliminarlos.

(Belcic, 2020a; NETSCOUT, s. f.-b; Paessler, s. f.)

3.3. Identificación de vulnerabilidades

3.3.1. Ataques a redes telefónicas

Una red telefónica es una red de telecomunicaciones que abarca una gran parte del área geográfica del planeta, es considerada un sistema complejo porque se usa para realizar llamadas telefónicas a cualquier parte del mundo en segundos. Los primeros teléfonos no eran muy diferentes de los actuales, sin embargo, su funcionamiento era completamente diferente, y había muy pocos países con acceso a ellos.

Los ataques a las redes telefónicas son realizados por phreakers, estos son personas que hackean cualquier tipo de sistema telefónico, usando técnicas de intercepción.

En las décadas de 1960 y 1970 fue el auge del phreaking. Durante los primeros años del surgimiento de este fenómeno, los phreakers se dedicaron a descifrar el funcionamiento de la telefonía, y a través de técnicas de ensayo y error obtuvieron los primeros resultados, como descubrir la forma en que se enrutaban las llamadas, esto lo hacían escuchando los patrones de tonos cuando se marcaba.

Para encontrar más información que les fuera útil, buscaban y leían los manuales técnicos de las empresas de telefonía, incluso buscaban en los botes de basura de las empresas documentos que les pudieran ser de utilidad.

Entre las primeras cosas que consiguieron los phreakers se encuentra que lograron hacer llamadas telefónicas en teléfonos de marcador de disco que estuvieran bloqueados, es decir, en teléfonos que tenían bloqueado el mecanismo para discar números, la técnica que usaron fue conocida como switch-hooking.

El funcionamiento de la técnica consistía en pulsar el gancho (switch hook) que hacía de tope repetidamente en intervalos regulares de tiempo y con una separación de un segundo entre las series se podían marcar números para realizar llamadas en los teléfonos que solo eran usados para recibir llamadas.

En el caso de los teléfonos con teclado se usaba un método diferente, se necesitaba un marcador antiguo de tonos, la función de este era imitar los sonidos que hacían las teclas al presionarlas cuando se marcaba un número, ejemplos de estos teléfonos se observan en la figura 3.10.

Figura 3.10. Teléfonos.

A. Teléfono de marcador de disco. *B. Teléfono de teclas*

También se descubrió que podían realizar llamadas gratuitas. En el cereal Capn' Crunch se incluía un silbato que podía emitir un tono cuya frecuencia era de 2,600 Hz, frecuencia que era usada para indicar que una llamada telefónica había terminado. Después de que se emitía el tono con la frecuencia de 2,600 Hz uno de los extremos de la línea se desconectaba y el lado que quedaba conectado entraba en modo operador, por lo que se podía explorar y hacer llamadas de forma gratuita. Un poco de tiempo después, las operadoras telefónicas notaron esto, por lo que empezaron a usar tonos multifrecuencia, lo que invalidaba el truco del silbato.

En las redes de telefonía tradicional, las líneas pertenecen a líneas conmutadas, las cuales se componen por un conjunto de nodos interconectados, y con ayuda de una central telefónica se establece una conexión permanente entre ambos nodos con la finalidad de comunicarlos.

Al momento de realizar una llamada, la red intenta establecer un canal fijo entre los dos nodos, si ésta logra realizarse se extiende entre los nodos un canal que se dedica a atender esa llamada en particular y no puede ser usado para realizar otra acción hasta que la llamada termine, es decir, en la telefonía tradicional es necesario tener una línea dedicada para realizar la llamada, ya que este tipo de redes no está diseñado para soportar tráfico de datos, solo de voz. Algo importante que hay que mencionar, es que el sistema de telefonía tradicional usa cables de cobre para transmitir las señales de voz.

Con el paso de los años la tecnología ha evolucionado para adaptarse al mundo que también ha estado en constante evolución, por lo que la tecnología se ha vuelto más eficiente y han surgido nuevas tecnologías como la telefonía IP.

La telefonía IP, también conocida como telefonía por internet usa la tecnología voz sobre IP (VoIP), la cual es una tecnología que permite convertir la voz analógica en digital, dicho de otra manera, VoIP es un canal de voz a través del cual se puede realizar una llamada en la red, esto quiere decir que la telefonía IP integra la trasmisión de voz y datos, que en un inicio se encontraban separados.

Entre la telefonía tradicional y la telefonía IP se tienen varias diferencias, entre las cuales se encuentran:

- En la telefonía IP los servicios de VoIP viajan a través de una red de datos e internet.
- En VoIP no hay restricción respecto a la cantidad de nodos conectados, esto permite que se puedan realizar llamadas con múltiples personas, contrario a la telefonía tradicional, en donde las llamadas se realizaban únicamente entre dos nodos.
- Con VoIP no importa donde se encuentren los interlocutores, podrán realizar una llamada siempre que tengan una red de datos y conexión a internet.
- VoIP además de permitir voz, también permite enviar multimedia, mensajería o documentos.
- Al usar VoIP una organización reduce costos, debido a que enviar voz a través de internet es menos costoso, comparado con la telefonía tradicional.

VoIP no está exento de los problemas de seguridad, al funcionar sobre IP también se expone a una serie de ataques con los cuales la información de la red puede verse comprometida:

- **Ataque de denegación de servicio (DoS o DDoS):** el servicio de VoIP también es vulnerable a este tipo de ataque. Para realizarlo, el atacante satura los dispositivos con paquetes TCP, enviando múltiples peticiones para agotar los recursos, también puede enviar peticiones para finalizar las llamadas.
- **Escuchas no autorizadas:** un atacante puede aprovechar algún servicio que esté mal configurado o que tenga vulnerabilidades las cuales pueda aprovechar para penetrar en el sistema, después de hacer esto, extrae el tráfico de la red para obtener las conversaciones del servicio de VoIP usando herramientas de sniffing, para posteriormente convertirlo en un archivo reproducible.
- **Spam VoIP:** este tipo de ataque se aprovecha de la ventaja de VoIP para realizar llamadas de manera simultánea, ya que se pueden realizar ataques que bloqueen las líneas telefónicas de una empresa, cortando canales de comunicación. Además, el estar recibiendo llamadas cada poco tiempo se ve afectada la productividad de los empleados, ya que deben atender todas las llamadas que se reciben, para verificar si alguna de ellas es fidedigna.
- **Vishing:** esta es una técnica de ingeniería social que se usa para conseguir información vía telefónica, esta técnica suele ser combinada con phishing, donde por medio de un correo electrónico se adjunta un número telefónico de alguien que no es quien dice ser, pero que casualmente coincide con la población de la empresa.

Hay muchos ataques que se puede realizar a VoIP, por lo que es importante que se encuentre protegido correctamente para que este tipo de telefonía no exponga a la organización a amenazas.

Para prevenir ataques a VoIP se tiene que implementar protección perimetral (tema 1.1.4), es decir, se tienen que implementar sistemas IPS, IDS, firewalls o análisis avanzado de protocolos. También hay tecnologías de protección perimetral que se especializan en VoIP.

Algo que también se tiene que tomar en cuenta es el cifrado, ya que esto puede prevenir un ataque que atente contra la confidencialidad de las conversaciones, para esto se puede hacer uso de VPN (Virtual Private Network o Red Privada Virtual), IPsec (Internet Protocol Security o Seguridad del Protocolo de Internet) o SRTP (Secure Real Time Transport Protocol o Protocolo de Transporte en Tiempo Real). También es importante elegir un algoritmo de cifrado que sea rápido y eficiente.

Es importante tomar en cuenta que los routers y switches deben de estar alineados con los procesos de seguridad de la organización, como que solo estén abiertos los puertos que se van a utilizar, también deben de estar configuradas las listas de control de acceso.

Algo importante que hasta ahora no se ha mencionado es que se debe de considerar la disponibilidad del servicio, hay que considerar que un corte de energía puede provocar que la red se caiga por lo que se sugiere que haya redundancia en la red o fuentes de respaldo que alimenten la red mientras se soluciona el corte de energía.

(Agudo, 2017; Agüero, s. f.; Lemus, 2020; Pedroza, 2021)

3.3.2. Ataques a la telefonía inalámbrica y telefonía celular

Un teléfono inalámbrico es una combinación de un teléfono y un transmisor de radio, consta de dos partes, una de ellas es la base y la otra el auricular. La base se conecta a la red de telefonía fija, y recibe las llamadas entrantes a través de la línea de teléfono, dichas llamadas las convierte en señales de radio FM y difunde la señal por el aire, el auricular recibe esta señal para convertirla a una señal eléctrica y la envía a través de un altavoz, donde se convierte en el sonido que escuchamos de manera habitual. Cuando una persona habla, el auricular difunde su voz por una señal de radio FM y la devuelve a la base, donde es convertida a una señal eléctrica y envía dicha señal por la línea de teléfono a la otra persona.

Este tipo de teléfonos aparecieron en la década de los 80 y operaban en una frecuencia de 27 MHz. Inicialmente tenían una serie de problemas, como, por ejemplo, un rango limitado, una calidad de sonido deficiente y con interferencia ocasionada por paredes y muebles. La seguridad de este tipo de teléfonos no era buena, ya que se podían interceptar las señales desde otro teléfono inalámbrico, esto debido al número limitado de canales.

A finales de esta misma década hubo una mejora en estos teléfonos, pues operaban a una frecuencia de 49 MHz con lo cual había menos interferencia y se necesitaba de menos energía para que funcionaran.

En el año de 1995 se introdujo la tecnología DSS cuya abreviación deriva del inglés Dynamic Spectrum Sharing, en español conocida como Compartición Dinámica del Espectro, este sistema permitía que la información digital se propagara en diferentes frecuencias entre el receptor y la base, esto hizo que fuera prácticamente imposible que se pudieran capturar las conversaciones ajenas.

La telefonía móvil o telefonía celular, es un servicio público de conexión a la red telefónica publica mediante una red inalámbrica, que tiene como objetivo facilitar la comunicación, la cual se lleva a cabo mediante ondas de radiofrecuencia, las cuales viajan a través del espectro radioeléctrico hasta llegar a su destino, por lo que se elimina la necesidad de usar conexiones físicas.

Este servicio recibe el nombre de móvil porque permite que la persona que hace uso del servicio se pueda desplazar de un lugar a otro, mientras que celular, hace referencia a la forma en como están planeados los sistemas celulares, ya que la zona de cobertura se divide en zonas más pequeñas, las cuales se llaman células o celdas.

En la figura 3.11 se puede observar que estas celdas tienen forma hexagonal, esto se debe a que con esa forma se puede ocupar todo el espacio, también se puede observar que en cada célula hay una estación base, la cual tiene la capacidad de enviar y recibir señales en su espacio designado.

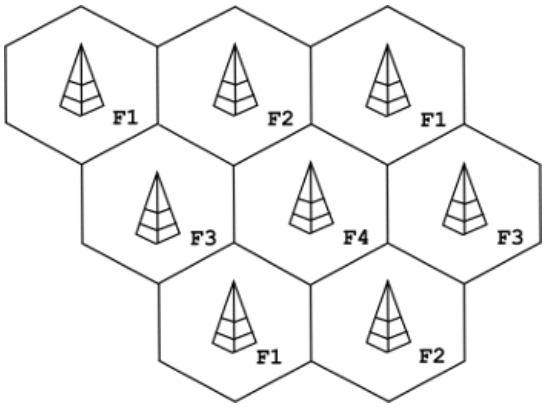


Figura 3.11. Celdas o células.

[Imagen]. Alegsa Leandro. Definición de red celular, (s.f.). https://www.alegsa.com.ar/Dic/red_celular.php#gsc.tab=0

La telefonía celular se compone de tres elementos:

- **Centro de conmutación móvil (CCM):** se puede decir que es el cerebro de todo el sistema celular, controla el enrutamiento de las llamadas, determina la ubicación de la EM (Estación Móvil) dentro del sistema, detecta y registra las EM visitantes, es decir, las EM que pertenecen a otra red, entre otras funciones más que realiza. Debido a que el CCM es el cerebro del sistema celular debe tener conexión permanente con todos los elementos de la red, para lograr esto se disponen de enlaces directos entre el CCM y las

EB (Estación Base), por lo general estos enlaces son de microondas o de fibra óptica y el CCM verifica el estado de los enlaces, lo que contribuye al buen funcionamiento del sistema.

- **Estación base (EB):** es la encargada de recibir y enviar señales desde y hacia las EM, así como determinar su intensidad, además es el elemento que envía las señales hacía el CCM.
- **Estación móvil (EM):** se refiere el teléfono móvil que brinda la capacidad de establecer una llamada.

Cuando una EM hace realiza una llamada, se conecta con el CCM de la EB más cercana, el CCM busca el destinatario correcto en la red de las estaciones base y una vez que lo encuentra conecta las dos estaciones base (emisora y receptora), emitiendo una alerta, la cual es el aviso de llamada en el teléfono receptor.

La diferencia entre un usuario de telefonía móvil y uno de telefonía celular se encuentra en que un usuario de un teléfono inalámbrico también es un usuario móvil pero únicamente dentro del área de cobertura de su propia estación base, los teléfonos inalámbricos tienen una cobertura de aproximadamente 30 metros en una zona con edificios y de aproximadamente 100 metros en una zona abierta.

Un usuario también puede ser víctima de un ataque a través de la telefonía inalámbrica. Hay una vulnerabilidad descubierta llamada ReVOLTE, la cual permite descifrar y escuchar llamadas que pasan por una misma estación base, esta vulnerabilidad se descubrió en el protocolo Voice over LTE.

Esta vulnerabilidad se produce porque a veces los operadores móviles usan la misma clave de cifrado para cifrar las llamadas que pasan por una misma estación base, lo que puede ser un problema si el atacante conoce la ubicación de la llamada y la estación base a la que se dirige, ya que podría escuchar el contenido de la llamada y descifrar el tráfico, siendo el problema principal que no hace falta que el tráfico se descifre en el mismo momento, ya que el atacante puede grabar la llamada y descifrar su contenido posteriormente.

Hay otros tipos de ataques de los que puede ser víctima un usuario mediante un dispositivo móvil o inalámbrico, puede ser víctima de ingeniería social mediante una llamada telefónica, de phishing, un escaneo a la red inalámbrica a la cual se conecta u otro tipo de ataques, como sniffing, ataques a DNS, suplantación de identidad, entre muchos otros ataques.

Hay que recordar que es importante mantener la seguridad en los dispositivos móviles con los que se cuenta, ya que estos almacenan una gran cantidad de información, de la cual un atacante podría obtener un beneficio si logra acceder a ella. En el caso de los dispositivos móviles, es recomendable proteger el acceso a la información que contienen utilizando los sensores biométricos con los que cuentan actualmente la mayoría de ellos, con uso de patrones o contraseñas, e incluso es importante que el dispositivo móvil tenga instalado un antivirus.

Asimismo, el usuario debe ser cuidadoso con las páginas a las que ingresa usando los navegadores web, ya que podría caer y entrar a páginas no legítimas y sufrir robo de información, tal como pasaría en una computadora, estas formas de ataque ya se mencionaron en el tema 3.1.

(Dorian, 2020; El Tiempo, 1994; Martín, 2020)

3.3.3. Barrido de puertos

Los puertos de red son una interfaz que sirve para comunicarse con un programa a través de la red, pueden verse como entradas a una computadora para ejecutar diferentes aplicaciones, cada uno de los puertos existentes tiene asignado un número, el cual puede ir de 0 a 65,535, dicho número sirve para identificar la aplicación que se está usando.

La IANA cuyas siglas significan Internet Assigned Numbers Authority conocida en español como Autoridad para Números Asignados en Internet, es la organización encargada de la asignación de estos puertos, por lo que los dividió en tres categorías:

- **Puertos bien conocidos:** se refiere a los puertos con números inferiores al 1,024, estos son puertos reservados para el sistema operativo y son usados por protocolos como HTTP (Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertextos), POP3 (Post Office Protocol o Protocolo de Oficina de Correo), SMTP (Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo), entre otros.
- **Puertos registrados:** son los puertos comprendidos entre 1,024 y 49,151, estos pueden ser usados por cualquier aplicación. Hay una lista publicada en la página web de la IANA donde se puede observar el protocolo que usa cada uno de ellos.
- **Puertos dinámicos o privados:** son los puertos que se encuentran comprendidos entre el 49,152 y el 65,535, estos regularmente son asignados de forma dinámica a las conexiones peer to peer.

El escaneo de puertos es un proceso mediante el cual se analizan los puertos de un sistema, al hacer esto se obtiene información, como saber cuáles son los puertos abiertos, cuáles son los que están cerrados o saber cuáles son los que están protegidos con un firewall.

El escaneo de puertos no siempre es legal, porque puede realizarse para diferentes cosas, entre ellas:

- El administrador del sistema puede realizarlo para conocer los servicios que ofrece el dispositivo o analizar el estado de los puertos. Asimismo, puede crear un mapa de conexiones para detectar vulnerabilidades y brechas de seguridad. En este caso el escaneo de puertos es legal.

- Por otro lado, un atacante puede realizar un escaneo para saber cuáles son los puertos abiertos y explotar las vulnerabilidades que encuentre, en este caso el escaneo de puertos es ilegal.

Para prevenir ataques de escaneo de puertos es necesario tomar medidas de seguridad, entre las cuales se encuentran:

- Realizar un escaneo de puertos para saber cuáles se tienen abiertos y mantener abiertos solo los que se van a ocupar, los que no hay que dejarlos cerrados.
- Usar un firewall para mantener la seguridad en los dispositivos del sistema.
- Usar un IDS para bloquear conexiones sospechosas.
- Mantener los dispositivos actualizados para tener los parches de seguridad que eviten que un atacante explote alguna vulnerabilidad existente.

De ser posible, se deben usar herramientas que detecten cuando se está realizando un escaneo de puertos, como, PortScanDetector, esta herramienta alerta a los administradores cuando han sido escaneados más de 10 puertos, ya que esto podría significar que un atacante está intentando acceder.

(Grupo Atico34, 2021b; NMAP, s. f.)

3.3.4. Identificación de firewalls

Un firewall es un elemento de hardware, software o basado en la nube, el cual monitorea el tráfico que pasa por una red, decide cual es el tráfico que deja pasar y cuál es el tráfico que bloquea, es decir, usa el filtrado de paquetes para proteger a las de redes de ataques como el barrido de puertos, esto de acuerdo a un conjunto de reglas de seguridad que tiene definidas.

- **Firewalls de hardware:** son dispositivos instalados en una red para levantar una defesa y así proteger la red del exterior, al ser dispositivos externos tienen la ventaja de que no necesitan ser configurados cada vez que se reinstala el sistema operativo en una computadora, además de que no consumen recursos del sistema, la mayor desventaja que pueden tener es que es complicado actualizarlos y configurarlos correctamente, aunque estos pueden resultar efectivos con muy poca o ninguna configuración, además de que protegen a todas las máquinas de una red local.
  Estos firewalls de hardware usan el filtrado de paquetes para examinar su cabecera y determinar cuál es su origen y cuál es su destino, esta información es comparada con el conjunto de reglas predefinidas, las cuales determinan si dejan o no pasar el tráfico.
- **Firewalls de software:** o firewalls personales son programas que filtran el tráfico que entra y sale de una computadora, y resultan más económicos que los de hardware, además su instalación y actualización es sencilla, pero, consumen recursos del equipo,

sin embargo, un buen firewall de software se ejecuta en segundo plano, usando solamente una pequeña parte de los recursos del equipo.

Este tipo de firewall ayuda a proteger el equipo de ataques externos que intenten obtener el control del equipo, incluso puede proporcionar protección contra virus, troyanos, y gusanos más comunes, también puede tener controles definidos para establecer una compartición segura de archivos e impresoras y así bloquear aplicaciones no seguras para impedir que se ejecuten.

Para usuarios poco familiarizados con el firewall, usar los de software es muy sencillo ya que se instalan como cualquier otro programa, y pueden configurarse de diferentes maneras, permitiendo así más control sobre su funcionalidad y sus características de protección, sin embargo, una desventaja de estos es que solo protegen al equipo en el que están instalados y no a la red entera como los firewalls de hardware, además algunas veces pueden ejecutarse incorrectamente, por lo que pueden causar errores de compatibilidad con algún otro software que este previamente instalado.

Tipos de firewall

Los firewalls se dividen en distintas categorías de acuerdo a su estructura general y la forma en la que operan:

- **Firewalls de filtrado de paquetes:** son los firewalls más básicos y antiguos, estos realizan una verificación de los paquetes de datos que ingresan a la red por medio del router, revisan el tipo de paquete, las direcciones IP destino y origen y número de puerto. Esta información es comparada con las reglas que tiene definidas, por lo que si no hay coincidencias el paquete es rechazado y no le permite el paso a la red.

  Una ventaja de estos firewalls es que no necesitan de muchos recursos, por lo que no impactan significativamente en el rendimiento del sistema, sin embargo, como desventaja tienen que pueden ser evitados muy fácilmente esto comparándolos con los firewalls más robustos.
- **Circuit level Gateway:** es otro tipo de firewall que permite o deniega de manera rápida el tráfico de la red, sin consumir muchos recursos del sistema. Los gateways a nivel circuito funcionan verificando el protocolo de enlace de TCP, el objetivo de este es garantizar que sea legítima la sesión de donde proviene el paquete.

  Este tipo de firewall es muy eficiente en cuanto a recursos, sin embargo, no hacen una verificación del paquete en sí, por lo que en dado caso de que se tenga el protocolo de enlace TCP correcto así contenga un malware pasará de inmediato, esta es una de las razones por las cuales este tipo de firewalls no son suficientes para proteger el sistema correctamente.
- **Firewalls de inspección de estado:** este tipo de firewalls combinan la tecnología empleada en los firewalls de filtrado de paquetes y la verificación del protocolo de enlace TCP con el fin de tener un mayor nivel de protección, esto trae como desventaja que se pueda hacer más lenta la transferencia de paquetes legítimos.

- **Firewalls proxy:** estos trabajan en la capa de aplicación, filtran el tráfico que entra, así como su fuente. Este tipo de firewalls no permite que el tráfico se conecte directamente, ya que lo primero que hace es realizar una conexión con la fuente que origina el tráfico, además inspecciona el paquete de datos que entra. El tipo de verificación que hacen los firewalls proxy es muy semejante a la que hacen los firewalls de inspección de estado, ya que realizan un análisis de los paquetes y el protocolo de enlace TCP, adicionalmente verifican el contenido real del paquete mediante una inspección de capa profunda. Después de que la verificación es completada, el proxy es quien envía el paquete, lo que hace que haya una separación entre el cliente y los dispositivos de la red, creando anonimato y protección adicional para la red.
  La desventaja de este tipo de firewall es que puede ralentizar la transferencia de manera significativa, por los procesos de verificación que realiza.
- **Firewalls de próxima generación:** los firewalls lanzados recientemente son los que se conocen como arquitecturas de próxima generación. Su función principal está destinada a detectar y bloquear ataques sofisticados a través de fortalecer las políticas de seguridad a nivel de aplicación, puertos o protocolos de comunicación. Este tipo de firewalls combina características de los firewalls tradicionales, además, añaden sistemas IPS, inspección de SSL y SSH, inspección profunda de paquetes y detección de malware basado en la reputación y conocimiento de la aplicación.
  Estos firewalls tienen como objetivo frenar el número de ataques e incluir más capas del modelo OSI. La diferencia más notable entre un firewall tradicional y uno de próxima generación es que los de próxima generación realizan una inspección más profunda de paquetes.
  Estos tienen como ventaja que pueden bloquear el tráfico antes de que ingrese a la red, además están mejor equipados para abordar las amenazas persistentes avanzadas, y ofrecen diferentes opciones que se ajustan a las necesidades de cada organización.

Tener un firewall no significa que la red va a estar protegida en todo momento, es importante combinarlo con otros componentes de seguridad para que la red se encuentre debidamente protegida. Algunas de las amenazas a las que se puede enfrentar un firewall son:

- **Ataques internos:** los ataques internos pueden deberse a que los accesos al sistema por parte de los trabajadores de la organización no son filtrados por el firewall, por lo que alguien dentro de la organización podría robar información, quedando esto lejos del área de defensa del firewall.
- **Ataques de virus sofisticados:** algunos firewalls proporcionan protección antivirus y antimalware, sin embargo, solo deben de considerarse en la primera línea de defensa y no como una barrera absoluta que protegerá la red en todo momento, por lo que algún atacante podría engañar al firewall y enviar un paquete con malware o virus, por eso también es importante tener instalado y actualizado un antivirus confiable.

Es muy común que los firewalls produzcan una falsa sensación de seguridad, ya que al instalarlo el administrador de la red tiende a despreocuparse sobre la seguridad de los demás dispositivos de la red. Al centralizar las medidas de seguridad en un mismo sistema, un atacante puede amenazar toda la red y aprovechar que ésta no se encuentra lo suficientemente protegida por no contar con protección adicional.

(E. Fernández, 2019a; Grupo Atico34, 2020c; Pérez-Roca Fernández & Pereira Suárez, s. f.)

3.3.5. Identificación de sistemas operativos / Fingerprinting

El fingerprinting también conocido como huellas digitales son pequeños patrones únicos que se forman en los dedos e identifican a una persona de manera única. Es una forma de biometría, donde se usan las características físicas de las personas para identificarlas.

El OS fingerprinting es una técnica que analiza las huellas dejadas por los sistemas operativos en sus conexiones de red, esto permite recopilar información del dispositivo para identificarlo y hacer un seguimiento de la actividad del usuario, esto está basado en los tiempos de respuesta de los paquetes al momento de que una conexión con el protocolo TCP/IP es establecida, en otras palabras, el fingerprinting es un proceso mediante el cual se recopila un conjunto de datos que permite identificar al dispositivo de manera única.

El fingerprinting no solo analiza y recopila los hábitos de navegación de los usuarios, hay técnicas avanzadas que son capaces de hacer un registro de los movimientos del mouse que hace el usuario a través de una página web. Los desarrollos para dispositivos como JavaScript o Flash facilitan la implementación de procedimientos para colectar información concreta del dispositivo, como el modelo del navegador, el tipo y versión del sistema operativo, arquitectura del procesador, dispositivos instalados, direcciones IP, entre otros. Si toda esta información obtenida se combina apropiadamente se puede crear una huella digital única del dispositivo que lo identifica de los demás usuarios de internet.

El OS fingerprinting tiene dos tipos, el activo y el pasivo.

- **Os fingerprinting activo:** se encarga de hacer que cada uno de los sistemas operativos responda de manera diferente a la variedad de paquetes que han sido malformados, para esto se usan herramientas que permiten comparar las respuestas con una base de datos especifica, la cual es usada como una referencia que permite identificar cual es el sistema operativo que está usando cada uno de los dispositivos objetivo.
  Este método es más directo y confiable porque hay una interacción directa con el sistema operativo objetivo, sin embargo, al hacer esta interacción se suele generar tráfico en la red donde opera el sistema operativo víctima, lo que puede generar sospechas.

- **OS fingerprinting pasivo:** este tipo de fingerprinting no actúa directamente sobre el sistema operativo del dispositivo objetivo, este mediante sniffing, analiza los paquetes que son enviados por el sistema operativo. Esto permite comparar cada uno de los paquetes con la base de datos que se tiene como referencia.
  Este tipo de fingerprinting es más silencioso, ya que no genera ningún tipo de tráfico, y solo intercepta los paquetes que viajan por la red del sistema operativo objetivo.

Para evitar que un atacante obtenga información usando esta técnica es recomendable implementar sistemas IDS, aunque muchas veces un sistema IDS puede no detectar el fingerprinting, a menos que sea un IDS reactivo, es decir un IDS que responda a la actividad sospechosa y reprograme los firewalls para bloquear el tráfico proveniente de la red del atacante.

Otra forma de evitar ser víctimas de un ataque de este tipo en sistemas operativos windows consiste en enmascarar el sistema operativo o modificar el valor de TTL (Time To Live o Tiempo de Vida), que en Windows es de 128 y podría modificarse por 64, que es el tamaño de TTL en Linux, también se puede modificar el tamaño de ventana de TCP/IP, así como desactivar los paquetes ICMP (Internet Control Message Protocol o Protocolo de Mensajes de Control de Internet) Redirects.

Para evitar estos ataques en sistemas operativos Linux se puede modificar el valor de TTL de 64 a 128, desactivar el TCP TIMESTAMP, desactivar el tamaño de la ventana y activar los paquetes ICMP Redirects.

Es recomendable que antes de hacer modificaciones se realicen copias de seguridad, ya que al modificar estos parámetros se puede ver afectada la conectividad del sistema y también pueden dejar de funcionar algunos servicios, por lo que si se quiere usar esta técnica se tiene que probar que los servicios que se ofrecen funcionen adecuadamente.

Otra forma de evitar este tipo de ataques es usar sistemas operativos virtuales, esta técnica no permite ocultar o cambiar completamente el sistema operativo, sin embargo, va a permitir ocultarlo en aspectos concretos de conexiones, para hacer esto se puede usar honeypots, el cual es un simulador que sirve como herramienta de seguridad, diseñado para obtener datos valiosos sobre los atacantes y sus métodos de ataque, así como las herramientas y técnicas que utilizan. También permite ocultar sistemas operativos reales en sistemas operativos virtuales, por lo que esta última técnica es la mejor opción para camuflar el sistema y evitar ataques de fingerprinting.

(Agencia Española Protección Datos, s. f.; IT Perfection, 2020; Paz, 2008; Zambrano, 2020)

3.3.6. Escaneo a redes inalámbricas

Una red inalámbrica es una red que está configurada para comunicarse por medio de ondas electromagnéticas las cuales son capaces de viajar por el espacio y de atravesar construcciones, este tipo de redes permite que los dispositivos permanezcan conectados sin la necesidad de usar cables.

De manera general, estas redes están formadas por un punto de acceso inalámbrico, también conocido como AP y es a este donde se conectan los dispositivos inalámbricos.

Para que un dispositivo se conecte a una red inalámbrica debe tener una tarjeta ethernet, esta tarjeta transforma los datos binarios manejados por la computadora en ondas de radio, las cuales se transmiten al dispositivo receptor a través de una antena, la cual está conectada en uno de los puertos de la tarjeta ethernet. El dispositivo receptor recibe los datos con su propia antena y los decodifica con ayuda de su tarjeta ethernet para que el dispositivo pueda entender los datos que ha recibido.

Si se quiere conectar una red a otra red o a internet se necesita de un router. El router recibe los datos del dispositivo receptor y los codifica en otros datos que sean capaces de viajar por la red que une a ambas redes que se quieren comunicar, esta unión puede ser alámbrica o inalámbrica, cuando los datos llegan a la red destino, el router decodifica los datos que recibe y los envía al dispositivo destino de su red.

Una forma de descubrir vulnerabilidades que un atacante puede aprovechar es realizando un escaneo de la red, este es un proceso donde se analizan los dispositivos que se encuentran actualmente conectados con el fin de detectar si hay algún tipo de vulnerabilidad, y con los resultados saber en qué estado se encuentra la seguridad de la red. Esta recolección de datos es muy útil para los atacantes ya que así pueden recopilar información de la red víctima para aprovecharla y obtener un beneficio propio, mientras que a los administradores de red les es de utilidad para encontrar esas vulnerabilidades antes de que el atacante pueda aprovecharse de ellas. El propósito de un escaneo de red por parte de los administradores es administrar, mantener y proteger el sistema de los posibles atacantes.

Hay dos tipos de escaneo de red, el escaneo de puertos visto en el tema 3.3.3 y el escaneo de vulnerabilidades, el cual, como su nombre lo indica, ayuda a encontrar las vulnerabilidades en una red, por lo que al realizar este tipo de escaneo se expondrán amenazas que estaban ocultas a simple vista, para los administradores de la red es mejor detectar dichas vulnerabilidades para poder corregirlas, antes de que un atacante las encuentre y se aproveche de ellas para atacar la red.

Hay diferentes herramientas con las cuales se puede realizar un escaneo de la red, entre las que se encuentran las que se listan a continuación:

- **SATAN – Security Analysis Tool fot Auditing Networks:** esta herramienta genera reportes automáticos de vulnerabilidades en sistemas remotos. Es un programa diseñado para los sistemas UNIX, y tiene que ejecutarse con privilegios de root. SATAN tiene un kernel en PERL y programas en C para la identificación de vulnerabilidades, también tiene programas de soporte en PERL, con los cuales controla búsquedas y generar reportes, además guarda los resultados en la base de datos.
- **COPS – Computer Oracle and Password System:** es una herramienta de seguridad que permite analizar sistemas UNIX, esto con el propósito de identificar problemas de seguridad. Este sistema está basado en scripts y programas en C, los cuales se pueden usar para hacer una evaluación del estado de la seguridad de muchos de los sistemas UNIX.
- **CPM – Check Promiscous Mode:** este es un programa que sirve para verificar si alguna de las interfaces de red del sistema está trabajando en modo promiscuo, ya que esto puede ser un indicador de que un hacker ha entrado al sistema e iniciado algún programa para interceptar los paquetes que viajan por ella.

Los escaneos de vulnerabilidades deben realizarse de forma regular, para descubrir las vulnerabilidades, poder corregirlas y así garantizar que el sistema junto con todo lo que contiene permanezca seguro.

(Cisco, s. f.-b; Redes Inalámbricas., s. f.)

3.3.7. Instalaciones físicas

En el tema 2.2 se mencionaron las vulnerabilidades físicas que puede haber dentro de una organización. Las vulnerabilidades físicas son aquellas que se encuentran en el lugar donde la información se está almacenando o manejando, por lo que es importante tener en cuenta la seguridad física del sistema para agregar una capa más de protección y aumentar la seguridad.

3.3.7.1. Seguridad de las instalaciones físicas

Hacer un análisis de las instalaciones físicas de una organización permite identificar las amenazas a las cuales está expuesta, ya que para proteger la información almacenada y los dispositivos que conforman el sistema las organizaciones deben proteger sus instalaciones.

Hay que tomar en cuenta tres áreas en la protección de instalaciones físicas:

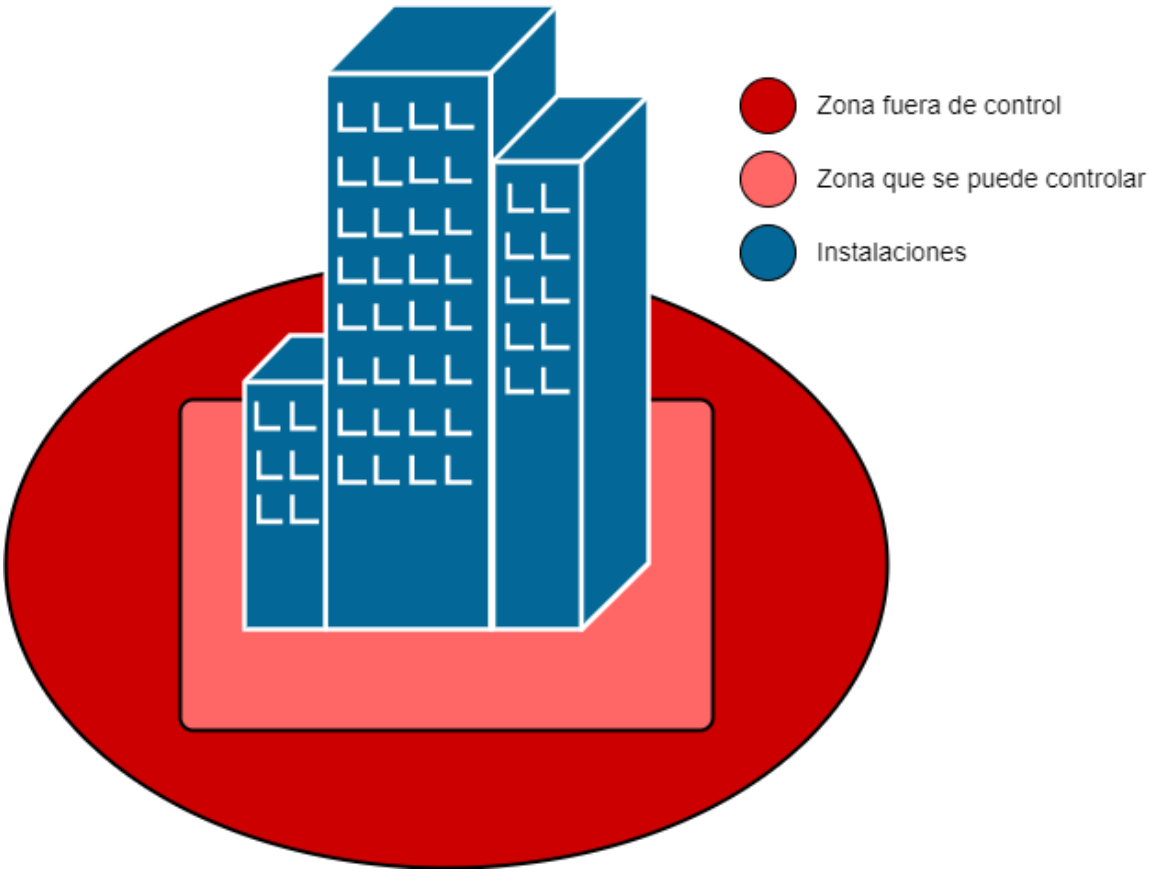


Figura 3.12. Instalaciones físicas.

- **Zona fuera de control**
  Es el área que rodea a las instalaciones, es importante identificar los riesgos que hay en esta área que puedan afectar las instalaciones de la organización. Dentro de esta zona se tiene que considerar:
  - El acceso a la oficina desde la calle.
  - Identificar si hay factores que pongan en riesgo las instalaciones desde la calle, por ejemplo, algún río cerca, coladeras en mal estado que no drenen bien el agua y puedan provocar alguna inundación dentro de las instalaciones, entre otros.
  - También hay que revisar si hay estructuras que puedan bloquear las comunicaciones satelitales de la organización.
  - También se deben identificar qué tipo de instalaciones rodean a la organización, para saber si en algún momento podrían representar un peligro para las instalaciones.
  - Adicionalmente, es indispensable identificar si en las inmediaciones de la organización existen áreas de riesgo para el personal que debe transitar por ahí a la llegada y a la salida de la organización y que pueden poner en peligro su seguridad.

Es importante identificar todos los factores externos a la organización, al no poder tener un control sobre los mismos sería imposible evitar que pasen acontecimientos que afecten directamente las instalaciones y al personal de la organización, sin embargo, al considerarlos se pueden tener medidas de emergencia para evitar afectaciones de los factores externos.

- **Zona que se puede controlar**

  Esta es un área que ya está bajo el control de la organización, aquí se debe de hacer un análisis para implementar algún tipo de seguridad perimetral, como la instalación de paredes externas, vallas o cercas que pongan un límite entre las instalaciones físicas de la organización y la zona que no se puede controlar. Adicionalmente, se tiene que hacer un análisis para verificar si las medidas implementadas afectan o no a los vecinos.

  En el área interna de la zona que se puede controlar, se tienen que considerar otros aspectos, como el control de acceso, es decir, se tiene que mantener un control de las personas que entran y salen de la organización, de igual manera se debe de considerar la entrada y salida de los vehículos. Para tener un buen manejo de esto se pueden usar controles de identidad y dividir las zonas de acuerdo a estos controles, es decir, tener un sistema de vigilancia en todos los accesos a la organización, además de dividir las zonas de acuerdo a los controles de identidad establecidos, es decir, se puede tener un área de estacionamiento exclusiva para trabajadores de la organización y otro exclusivo para visitantes o proveedores.

  También se deben de considerar las salidas de emergencia para hacer una correcta evacuación en caso de ser necesario, asimismo hay que tener vigilados los espacios abiertos que se tengan en esta zona controlada para evitar que algún tipo de incidente ocurra.

- **Instalaciones**

  Mantener seguridad en las instalaciones de la organización es muy importante, ya que es aquí donde se almacenan los activos de la organización. El diseño del edificio también juega un papel importante, ya que el diseño debe ser adecuado para poder enfrentar también los desastres naturales.

  La seguridad del edificio se debe tomar en cuenta desde que se accede directamente a él, por lo que se debe de implementar seguridad en puertas y ventanas, con el objetivo de evitar accesos no autorizados, al mismo tiempo se debe de contemplar que estas medidas implementadas no impidan la salida del personal en caso de que se tenga que hacer una evacuación de emergencia.

  Se debe de tener un procedimiento de control de acceso tanto al edificio, como a las áreas internas de la organización, como son los cuartos de equipos y

telecomunicaciones, así como oficinas del personal con altos cargos donde también se almacena información importante, esto para que todas las personas que necesiten acceder a estas áreas pasen por dicho procedimiento y así evitar que se haga un mal uso de las instalaciones.

Otro tipo de medidas que se pueden implementar es tener claramente señalizadas las rutas de evacuación, y de ser necesario se puede tener un área del edificio especial equipada con suministros de emergencia donde se pueda resguardar el personal en caso de ser necesario.

Es importante identificar bien estas tres áreas para implementar seguridad a las instalaciones que contemplan el hardware y la infraestructura, así como también a todo el personal que forma parte de manera directa o indirecta de la organización.

(EISF, 2014; Garijo, 2019)

3.3.7.2. Normas de cableado estructurado

El cableado estructurado es el cableado de un edificio o de un conjunto de edificios que permite interconectar equipos, para integrar diferentes servicios como datos y telefonía. Este cableado permite la administración sencilla de la red, además soporta muchos productos de telecomunicaciones sin ser modificado.

Para realizar este cableado, se hace uso de una serie de nomas sobre cableado estructurado, estas son establecidas por las siguientes organizaciones:

- **TIA – Telecommunication Industry Association o Asociación de Industrias de Telecomunicaciones:** esta organización fue fundada en 1985, se dedica al desarrollo de normas de cableado industrial para los productos de telecomunicaciones.
- **ANSI – American National Standards Institute o Instituto Nacional Estadounidense de Estándares:** organización sin fines de lucro la cual se encarga de supervisar como es que se desarrollan los estándares para productos, procesos y sistemas de EE.UU.
- **EIA – Electronic Industries Alliance o Alianza de Industrias Electrónicas:** esta organización promueve el desarrollo de competitividad en el sector de la tecnología de EE.UU.
- **ISO – International Standards Organization u Organización Internacional de Normalización:** la actividad principal que realiza esta organización es la elaboración de normas técnicas internacionales, con el objetivo de establecer niveles de homogeneidad en relación con la administración de servicios y desarrollos de productos en la industria.
- **IEEE – Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos Electrónicos:** es una organización dedicada a promover los avances científicos en la ingeniería eléctrica, electrónica, energética, informática y afines.

Las normas ANSI/EIA/TIA son normas relacionadas con el cableado estructurado, las cuales promueven que los dispositivos de red estén en lugares seguros y no cerca de zonas que puedan representar un riesgo, como elevadores, baños y sótanos. Los estándares que se usan con mayor frecuencia son:

- **ANSI/EIA/TIA 569:** el objetivo de este estándar es normalizar la práctica de diseño y construcción para canalizaciones dentro de edificios, principalmente comerciales. Además, reconoce tres conceptos que son fundamentales y que tienen relación con las telecomunicaciones y los edificios:
    - **Los edificios son dinámicos:** los edificios pueden cambiar para adecuarse a las nuevas necesidades de la organización.
    - **Los sistemas de telecomunicaciones son dinámicos:** es decir, durante la existencia del sistema los equipos de telecomunicaciones evolucionan, hecho que este estándar reconoce.
    - **Las telecomunicaciones son más que voz y datos:** las telecomunicaciones además de voz y datos incorporan otros sistemas como la seguridad, audio, video, alarmas y sonido, es decir, dentro de las telecomunicaciones se incorporan los sistemas de bajo voltaje que transportan información por todo el edificio.

  Este estándar es el central al momento de diseñar un sistema de cableado estructurado, esto se debe a que su enfoque principal son las rutas y espacios donde se instala el sistema de cableado, además permite generar un diseño donde las rutas sean óptimas para cada uno de los subsistemas, por medio de la especificación de materiales, ductos y prácticas de instalación.
  Al seguir las especificaciones de este estándar se tendrá un diseño óptimo que cubra todas las áreas de cableado, además de permitir la adecuación de los estándares a una infraestructura dada.

(López Villalvazo., 2004a)

- **ANSI/EIA/TIA 568A:** este es el estándar que especifica los requisitos mínimos para el cableado en establecimientos comerciales, se hacen recomendaciones para los requisitos mínimos del cableado para telecomunicaciones, como la distancia máxima de los cables, el rendimiento de los componentes y las topologías.
  Se pretende que el cableado de telecomunicaciones soporte varios tipos de edificios y aplicaciones de usuario, así mismo el tiempo especificado de vida útil de los sistemas de cableado es de mínimo 10 años. Este estándar fue reemplazado por la norma ANSI/TIA/EIA 568B.

- **ANSI/EIA/TIA 568B:** es otro estándar de cableado, donde se especifican los requisitos de cableado para edificios comerciales con soportes multiproducto y multimarca, también incluye información para el diseño de productos de telecomunicaciones.
  Esta norma está dividida en tres partes:
  - **ANSI/TIA/EIA 568 B1:** incluye el cableado genérico de telecomunicaciones en edificios comerciales, contiene requisitos y recomendaciones en estructura, configuración de interfaces, instalación, parámetros de desempeño y verificación.
  - **ANSI/TIA/EIA 568 B2:** se incluyen los requerimientos generales para componentes de par trenzado.
  - **ANSI/TIA/EIA 568 B3:** se especifican los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica.

  Los criterios que ofrece este estándar al aplicarse pueden incrementar el rendimiento del sistema de cableado, de manera que, aplicándolo correctamente, este estándar garantiza una vida útil de hasta 10 años.

(Gobierno del Estado de Tabasco, s. f.)

- **ANSI/EIA/TIA 606:** es un estándar de gestión para la infraestructura de telecomunicaciones de los edificios comerciales, este estándar tiene como propósito brindar un esquema de administración uniforme, el cual sea independiente de las aplicaciones, debido a que éstas pueden cambiar durante la vida útil del edifico.

(López Villalvazo., 2004b)

Las soluciones de cableado estructurado son fiables y seguras, ya que no solo mantienen la seguridad de la información que viaja por la red, sino que también proporcionan seguridad al personal.

La instalación del cableado estructurado puede hacerse en cualquier empresa, sin importar su tamaño, ya que los estándares se pueden adaptar a la infraestructura de la organización y ofrecer soluciones a las necesidades de cada cliente.

(Rubio Díaz, 2019; Unitel., 2013)

3.3.8. Configuración de servicios y servidores

Un servidor es un dispositivo o programa de software que almacena, distribuye y suministra información, y funcionan con la arquitectura “cliente servidor”, donde el cliente puede ser una computadora o aplicación que requiere información del servidor para funcionar, el servidor proporciona la información demandada por el cliente siempre y cuando el cliente esté autorizado.

Los tipos de servidores son:

- **Servidores de software:** son programas que proporcionan un servicio o respuesta a otros programas o a los usuarios.
- **Servidores de hardware:** son dispositivos donde se ejecutan programas o aplicaciones que responden a solicitudes de los usuarios.

Clasificación de servidores

Los servidores se clasifican de acuerdo al rol que desempeñan:

- **Servidor web:** este tipo de servidor almacena y organiza el contenido de las páginas web, proporciona la información al usuario a través de un navegador web, usando el protocolo HTTP.
- **Servidor DNS:** este tipo de servidor se encarga de relacionar una dirección de dominio con su respectiva dirección IP.
- **Servidor de correo electrónico:** este tipo de servidor se encarga de administrar el flujo del correo electrónico de los usuarios, permitiendo que se guarden, envíen o reciban correos electrónicos. Estos servidores hacen uso de protocolos como POP3 (Post Office Protocol o Protocolo de Oficina de Correo), SMTP (Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo) y IMAP (Internet Message Access Protocol o Protocolo de Acceso a Mensajes de Internet).
- **Servidor FTP (File Transfer Protocol o Protocolo de Transferencia de Archivos):** este servidor permite transferir archivos entre un cliente y un servidor, a diferencia del servidor de correo electrónico, el servidor FTP puede verse como un sistema cuyo objetivo es proveer datos en una red TCP/IP, sin embargo, los datos que son transmitidos se comparten en claro y para mantener la secrecía de la información se contemplan sistemas criptográficos de manera que entonces se trata de servidores SFTP. Este tipo de servidores es más común encontrarlos en equipos de organizaciones grandes por la gran cantidad de archivos que manejan.
- **Servidor de base de datos:** este tipo de servidor almacena bases de datos, además provee servicios de consulta y gestión a los clientes que quieren acceder a dichas bases de datos.

Aspectos a tomar en cuenta para la instalación de servidores

La instalación de un servidor va a depender del uso que se le quiera dar, al conocer las necesidades de la organización será más fácil elegirlo. No hay que olvidar que los servidores forman parte fundamental del sistema, ya que es en estos en donde se podrán gestionar los usuarios y contraseñas, también va a permitir establecer políticas de seguridad para la administración de las mismas.

Otro aspecto que se debe tomar en cuenta es el dispositivo donde se instalará el servidor, para esto es necesario considerar:

- La cantidad de usuarios que recibirá por día.

- El tipo de contenido de servicio que va a proporcionar el servidor.

Teniendo estos dos aspectos en cuenta es posible estimar las características que deberá tener el dispositivo que será el servidor, es decir, determinar la cantidad de memoria RAM, espacio de almacenamiento y la capacidad de procesamiento. También se debe tomar en cuenta que se deben de abrir los puertos del router que sean necesarios para que el servidor pueda comunicarse. Otro aspecto a considerar es la configuración del firewall, ya que se tienen que crear reglas apropiadas para que los usuarios puedan acceder al servidor y este se mantenga seguro.

Después de que el servidor fue instalado y configurado hay que realizarle mantenimiento, ya que esto ayudará a que el servidor funcione siempre de manera óptima, además de permitir detectar fallos a tiempo para evitar que se vea afectada la disponibilidad del servicio que proporciona.

Para determinar la frecuencia con la que debe realizarse el mantenimiento pueden usarse tres métodos:

- **Métodos estadísticos:** no suelen ser métodos muy usados ya que rara vez se tienen datos suficientes para realizar estudios estadísticos adecuados para determinar la frecuencia del mantenimiento.
- **Modelos matemáticos:** con este tipo de modelos se puede determinar la vida útil de una pieza o dispositivo para reemplazarlo antes de que presente algún problema, sin embargo, al igual que los métodos estadísticos, muchas veces es difícil tener un modelo de este tipo. Cabe mencionar que, en este sentido, lo más recomendable sería considerar las recomendaciones proporcionadas por el fabricante.
- **Experiencia de técnicos especialistas en mantenimiento:** es la manera más común para determinar la frecuencia de mantenimiento, ya que como su nombre lo indica, este tipo de método está basado en experiencias previas.
  Para determinar la frecuencia usando este método se puede hacer de dos formas:
  - Poniendo un determinado tiempo fijo entre cada una de las revisiones, para que las revisiones se realicen de manera periódica.
  - Realizando revisiones después de que han transcurrido ciertas horas de funcionamiento efectivo.

Usar alguna de las formas anteriores para determinar la frecuencia de mantenimiento es válido, incluso puede ser una combinación de los métodos y modelos mencionados.

Adicionalmente se tiene que diseñar una estrategia de backup, esto es fundamental para que en caso de que el servidor sufra un incidente no se pierda la información que éste almacena.

Se tiene que monitorear la carga que recibe el servidor, para tomar las medidas necesarias cuando éste reciba muchas solicitudes y no pueda atenderlas todas, así se evitará que el servidor deje de funcionar debido a la sobrecarga de solicitudes recibidas.

Como mencionan los estándares de cableado estructurado (tema 3.3.7.2) los dispositivos de los sistemas de comunicaciones son dinámicos, por lo que hay que considerar que en algún momento el sistema puede escalar las necesidades a cubrir y por ende se debe hacer una migración del servidor, esto porque el actual ya no es capaz de atender toda la demanda de solicitudes y necesita ser reemplazado por uno que satisfaga las nuevas necesidades de la organización.

Además, es necesario estar pendientes de las actualizaciones de seguridad, para evitar que por falta de algún parche de seguridad el servidor sea vulnerado, poniendo en riesgo los datos que almacena o la disponibilidad del servicio que ofrece.

(Bituser, 2016; J. L. Martínez, 2018; TIC Portal, 2023)

3.3.9. Software

El software es un elemento intangible que le permite a un sistema realizar determinadas funciones.

El software se clasifica de acuerdo a su función:

- **Software de programación:** se refiere a los programas informáticos que se usan para el desarrollar nuevo software, dentro de estas herramientas se incluyen los compiladores, los intérpretes y los editores de texto.
- **Software de sistema:** es el programa que ejecuta de las herramientas necesarias para que el sistema opere correctamente. Algunos ejemplos de software de sistema son:
    - **Cargadores de programas:** son los que se encargan de ejecutar otros programas, también se encargan de garantizar la estabilidad del sistema.
    - **Sistemas operativos:** este tipo de software incluye programas que permiten el manejo de memoria, medios de almacenamiento y administración de los diferentes periféricos, como el teclado, mouse, impresora, entre otros. Otra de las funciones del sistema operativo es servir de interfaz para el usuario.
    - **BIOS:** este realiza funciones básicas de arranque, control, identificación y configuración del hardware. Además, es responsable de la administración de flujo de datos entre el sistema operativo de la computadora y de los dispositivos conectados a esta.
- **Software de aplicación:** se incluyen los programas que no tienen que ver con el funcionamiento de la computadora, sino son los programas que se instalan en la computadora para ser usados como herramientas de trabajo, por ejemplo, procesadores de texto, programas de edición, videojuegos o navegadores de internet, entre otros.

En el software también se pueden encontrar vulnerabilidades, como:

- **Desbordamiento de búfer:** esta vulnerabilidad ocurre cuando en el código se usa un búfer de longitud fija y la aplicación intenta almacenar datos de una longitud mayor a la que soporta el búfer, esto trae como consecuencia que los datos se sobrescriban y se generen errores de segmentación. En estos casos, la programación segura evita que haya un desbordamiento haciendo uso de memoria dinámica.
- **Desbordamiento de enteros:** esto ocurre cuando el resultado de una operación es más grande que el tipo de variable donde será almacenado, por lo que el número que almacena es incorrecto, lo que provoca graves errores.

De acuerdo con lo anterior, con el software de programación se puede desarrollar nuevo software, pero para esto se debe de tener cuidado, ya que un atacante puede aprovechar algún error en la programación y lanzar un ataque, para evitar esto debe usarse la programación segura.

La programación segura se encarga de estudiar el nivel de seguridad del código fuente del software, su propósito es hallar y solucionar errores, para que éste sea lo más seguro y estable posible.

Algunos aspectos de los cuales se encarga la programación segura son:

- Utilización segura de funciones para evitar que la pila se desborde.
- Declaración segura de las estructuras de datos.
- Análisis profundo del software mediante testeos para detectar errores y posteriormente la creación de parches de seguridad para corregirlos.
- Uso de criptografía y de otros métodos de cifrado para evitar que los programas de software sean crakeados.

Generalmente, las organizaciones son las que definen las pautas de programación segura, por lo que puede formar parte de las políticas de la organización o pueden establecerse criterios que satisfagan los requerimientos de seguridad del proyecto que se está desarrollando.

Algunas de las buenas prácticas que se pueden usar para realizar programación segura son:

- Definir los requerimientos de seguridad en las primeras etapas del proyecto, esto porque las pautas de seguridad y programación deben establecerse de acuerdo a los requerimientos predefinidos y especificaciones del software.
- Hacer un modelo de simulación de todas las amenazas conocidas, el cual tiene que indicar los riesgos potenciales, asimismo debe indicarse una estrategia para proteger el código de dichos riesgos.
- Validar los tipos de entrada y bloquear los que no sean de utilidad, esto para garantizar que no se ingresen datos que puedan dañar el sistema, esto debido a que una fuente común de vulnerabilidades se encuentra en los datos que introducidos por el usuario.

- Mantener un diseño simple, ya que los diseños complejos aumentan las posibilidades de tener vulnerabilidades, además de que es más complicado identificar y corregir los errores.
- Usar herramientas que generen código automáticamente, esto porque dichas herramientas se pueden configurar para seguir políticas de programación segura, y por lo general no contienen errores humanos, lo que aumenta considerablemente la seguridad en el código.

Hay herramientas y metodologías que se pueden usar para evitar o minimizar el riesgo de vulnerabilidades asociadas al desarrollo de código, dentro de estas herramientas se encuentran los analizadores estáticos, las guías y metodologías completas para la programación segura.

Analizadores estáticos

Un análisis estático de código a veces es necesario para cumplir con estándares de seguridad y calidad del software, el análisis estático se define como el proceso de evaluar el software sin ejecutarlo, y con evaluación se refiere a la ejecución de algún mecanismo con el que se pueda extraer información de valor del código fuente, esta información puede ser útil para el equipo de desarrollo o el equipo de auditoría.

Dentro de los analizadores estáticos se encuentran:

- **PMD:** esta es una herramienta que se encarga de validar los estándares de construcción del código, es decir, evalúa la sintaxis del código fuente para encontrar incidencias de un determinado problema que haya sido previamente configurado para ser detectado. Esta herramienta funciona para lenguajes como Java, JavaScript, XML y XSL.
- **Flawfinder:** es un programa que examina el código fuente de C/C++, informa de las posibles fallas que pueda tener el código de acuerdo a su nivel de riesgo. Es útil para encontrar y eliminar rápidamente algunos problemas de seguridad antes de que el desarrollo se publique.
- **LAPSE:** esta herramienta está diseñada para ayudar a auditar aplicaciones Java para tipos comunes de vulnerabilidades encontradas en aplicaciones web.

Hay otras herramientas comerciales que suelen funcionar para diferentes lenguajes de programación, como CodeSecure, AppScan y Fortify.

Guías

También existen diferentes guías que recopilan buenas prácticas de programación para el desarrollo de aplicaciones seguras:

- **ISO Programming languages:** proporciona una guía para el uso del lenguaje Ada en sistema de alta integridad.
- **MISRA – The Motor Industry Software Reliability Association o Asociación de Fiabilidad del Software en la Industria del Motor:** proporciona pautas de buenas

prácticas para la aplicación segura de sistemas de control integrados y software independiente.

- **OWASP – Open Web Application Security Project o Proyecto Abierto de Seguridad de Aplicaciones Web:** es una organización sin fines de lucro que está dedicada a la búsqueda de vulnerabilidades en el software.

Metodologías de programación segura

Al hablar de metodologías de programación segura se encuentran:

- **The Software Security Framework:** es un conjunto de prácticas fundamentales para el desarrollo de software, seguir dichas prácticas ayuda a reducir el impacto potencial de la explotación de las vulnerabilidades no detectadas, y evita que se repitan.
- **OWASP SAMM – Software Assurance Maturity Model o Modelo de Madurez del Aseguramiento del Software:** este es un modelo que ayuda a las organizaciones a implementar estrategias de seguridad del software, las cuales se adaptan a los riesgos específicos que enfrenta la organización.
- **Microsoft SDL – Microsoft Security Development Lifecycle:** también conocido como Ciclo de Vida de Desarrollo de Seguridad de Microsoft, presenta consideraciones de seguridad y privacidad en las fases de desarrollo, esto permite que los desarrolladores creen software altamente seguro, aborda los requisitos de seguridad al mismo tiempo que los costos de desarrollo se ven reducidos.

Como se puede observar, hay diferentes herramientas que ayudan a mejorar la seguridad en los desarrollos de software, es importante conocerlas ya que son de utilidad para minimizar los riesgos que puedan surgir.

(CILSA, s. f.; DragonJAR, s. f., 2008; DWheeler, s. f.; Etxahun, s. f.; GCFGlobal.org, s. f.; HP, 2021; ISO, s. f.; Junta de Andalucia, s. f.-b; NIST, 2021; OWASP.org, s. f.; Universidad Internacional Valencia, 2022)

3.3.10. Hardware

El hardware hace referencia a la parte física y por lo tanto tangible de un sistema informático, entre los elementos físicos se incluyen los componentes eléctricos, electrónicos, electromecánicos y mecánicos.

El hardware se clasifica en las siguientes categorías:

- **Hardware de procesamiento:** son todos los componentes que tienen la capacidad de realizar operaciones lógicas, o dicho de otra manera, son los componentes que pueden procesar la información que es ingresada por los usuarios, por ejemplo, un microprocesador o una tarjeta de red.

- **Hardware de almacenamiento:** hace referencia a todos los componentes que le permiten a los usuarios, programas y procesos guardar información y es posible recuperarla en procesos posteriores. El hardware de almacenamiento puede estar incluido dentro de los dispositivos como un disco duro, o también pueden ser soportes portátiles, como una memoria USB.
- **Dispositivos periféricos:** hace referencia a todo tipo de hardware que permite que haya una comunicación entre los sistemas y los humanos. Los dispositivos periféricos se dividen en:
    - **Dispositivos periféricos de entrada:** son los dispositivos que permiten introducir información a la unidad de procesamiento del sistema o computadora, como un teclado, un micrófono o una cámara.
    - **Dispositivos periféricos de salida:** son los dispositivos que permiten que un usuario recupere información de la computadora o sistema, por ejemplo, un monitor, un proyector o una impresora.
    - **Dispositivos periféricos de entrada y salida:** hace referencia a los dispositivos que permiten la entrada y salida de información, por ejemplo, un monitor táctil.

Es importante que el hardware también cuente con medidas de seguridad, por ejemplo, tener un control de acceso para que solo usuarios autorizados tengan permitido están en contacto cercano con el hardware, de no ser así, los dispositivos de hardware podrían sufrir algún tipo de daño físico que afecte su funcionamiento e incluso podrían ser robados si no cuentan con suficiente protección.

El hardware también tiene vulnerabilidades que ponen en riesgo la información que almacenan, entre las cuales se encuentran:

- **Rowhammer:** es una vulnerabilidad de las memorias RAM la cual se debe a la forma en la que actualmente se fabrican éstas memorias, ya que tienen una mayor capacidad de almacenamiento mientras que su tamaño es más reducido, esto tiene como consecuencia que no haya un buen aislamiento entre los componentes de la memoria, ya que se encuentran soldados unos muy cerca de otros, debido esta cercanía los componentes interactúan eléctricamente entre sí provocando un bit flipping, es decir, que los bits se inviertan, de 0 pasen a 1 y de 1 pasen a 0. Esta vulnerabilidad puede permitir a los delincuentes la obtención de contraseñas y al combinarla con otros ataques incluso podrían acceder al contenido de la memoria.
- **BadUSB:** USB tiene muchos usos, ya que además de memorias USB dispositivos como cámaras o teclados cuentan con un cable USB. BadUSB aprovecha una vulnerabilidad del firmware USB, cuando un dispositivo USB se conecta se realiza un proceso de inicialización, en dicho proceso se identifica el dispositivo junto con las clases a las que pertenece para que se carguen los drivers necesarios y el dispositivo funcione correctamente. Para aprovechar esta vulnerabilidad, los atacantes modifican el firmware del USB, añadiendo funciones adicionales como ejecutar comandos, exploits, virus,

malware o algún otro programa malicioso de forma discreta, incluso una memoria externa USB podría reprogramarse para que actúe como un dispositivo de red, por lo que todo el tráfico de la red pasaría por la memoria, poniendo en riesgo toda la información de la víctima.

- **BIOS:** la BIOS es un firmware almacenado en una memoria no volátil la cual está integrada en la placa base de una computadora. La BIOS se encarga de que todo el hardware del dispositivo trabaje en conjunto correctamente para comenzar a cargar el sistema operativo. Un atacante puede usar un exploit para infectar la BIOS de un sistema y tomar el control por completo. Este tipo de ataque es muy difícil de detectar, ya que el código malicioso no es detectado por software antivirus y además sobrevive a los reinicios y renovaciones del firmware, sin embargo, si un atacante tiene éxito instalando el código malicioso está atacando todo el hardware, por lo que todo el sistema queda gravemente comprometido, ya que el atacante tendría acceso a toda la información confidencial, lo que es un gran riesgo de seguridad.

Las vulnerabilidades y ataques al hardware son bastante peligrosos, ya que como se vio anteriormente son muy difíciles de detectar, por lo que hay que poner atención especial para evitar que un atacante aproveche las vulnerabilidades del hardware y ponga en riesgo toda su información.

(Gómez, 2015)

3.4. Explotación y obtención de acceso a los sistemas de redes

3.4.1. Introducción a Metasploit

Metasploit es un proyecto de código abierto, el cual puede usarse con el objetivo de encontrar y explotar vulnerabilidades de un sistema, como es de código abierto puede personalizarse y usarse en muchos sistemas operativos.

Fue desarrollado en 2003 por HD Moore, inicialmente se desarrolló como una herramienta de red portátil, la cual estaba basada en el lenguaje de programación Perl, posteriormente, en el año 2007 HD Moore reescribió metasploit en Ruby y en al año 2009 fue adquirido por Rapid7, quienes desarrollaron una edición comercial a la cual llamaron Metasploit Pro.

Metasploit contiene una gran variedad de exploits. Un exploit es un programa, aplicación, cadena de código o secuencia de comandos que permite a quien lo usa, investigar y aprovechar las vulnerabilidades de un sistema. Los ciberdelincuentes suelen usar metasploit para identificar y explotar las vulnerabilidades del sistema víctima, mientras que los equipos de seguridad lo usan para realizar pruebas de penetración, y así identificar las vulnerabilidades existentes en el sistema.

Arquitectura de metasploit

La arquitectura de esta herramienta puede observarse en la figura 3.13:

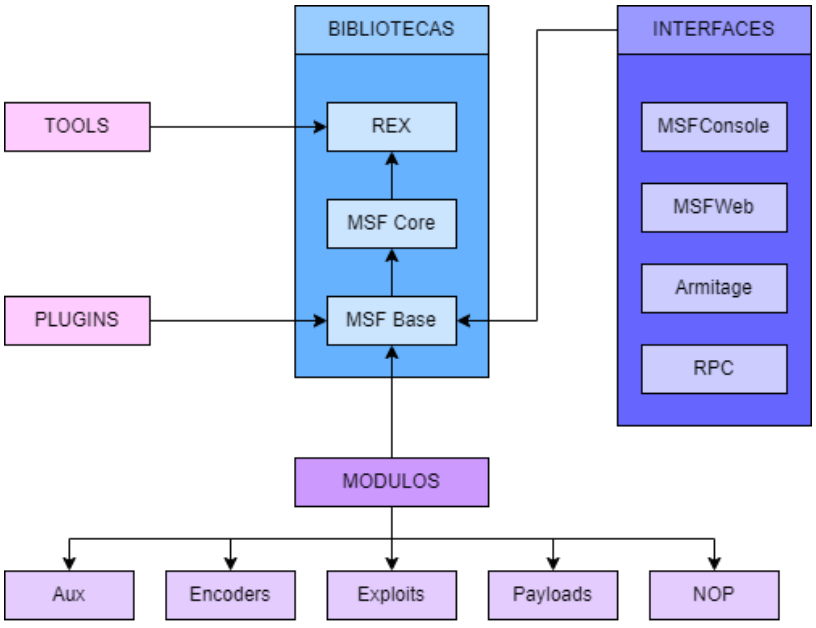


Figura 3.13. Arquitectura de Metasploit

(Arquitectura de metasploit., 2019)

- **Interfaces:** son las plataformas por las cuales se puede tener acceso a metasploit. Hay cuatro interfaces disponibles:
    - **MSFConsole:** es el tipo de interfaz más usada, permite el acceso mediante una interfaz de línea de comandos activa.
    - **MSFWeb:** permite acceder a metasploit usando una interfaz basada en navegador.
    - **Armitage:** interfaz gráfica de usuario que se basa en java, ésta permite la administración de ataques y la colaboración de los equipos de seguridad.
    - **RPC (Remote Procedure Call):** los usuarios mediante programación pueden hacer uso de metasploit, usando servicios de RPC basados en HTTP, además estos servicios pueden operar mediante lenguajes de programación como Java, Python y C.

- **Bibliotecas:** permiten a los usuarios ejecutar exploits, sin que tengan la necesidad de escribir código adicional. Metasploit tiene tres bibliotecas:
    - **REX:** permite habilitar las tareas más básicas, como la configuración de sockets, además, contiene Base64, HTTP, SMB, SSL y Unicode.
    - **MSF Core:** proporciona una API básica que contiene rutinas, con ésta se pueden desarrollar programas y herramientas.
    - **MSF base:** es donde se encuentra la configuración y los recursos de metasploit.

- **Módulos:** estos se usan para realizar diferentes tareas, se clasifican en:
    - **Payloads:** un payload es la parte del malware que se encarga de hacer las acciones maliciosas en el sistema, es decir, puede borrar datos o enviarlos al exterior, entre otros.
    - **Exploits:** es el programa que ejecuta una serie de comandos con el objetivo de aprovechar las vulnerabilidades del sistema, además los exploits son los que permiten ejecutar los payloads.
    - **Encoders:** ocultan los payloads para garantizar que se entreguen correctamente y eviten ser detectados por los antivirus, los IPS e IDS.
    - **NOP:** generan secuencias aleatorias de bytes para evitar los IPS e IDS.
    - **Aux:** proporciona herramientas externas, entre las cuales se incluye el escaneo puertos, vulnerabilidades, sniffers, entre otros.
- **Tools y plugins:** amplían la funcionalidad de metasploit.

Usos de metasploit

Metasploit es una herramienta que puede ser usada por los equipos de seguridad para simular escenarios de ataque y así descubrir las posibles vulnerabilidades del sistema y poder corregirlas, sin embargo, es importante tener presente que también puede ser usada por los

delincuentes informáticos para explotar vulnerabilidades de los sistemas, y obtener un beneficio de ello. Entre los usos que ofrece metasploit se encuentran:

- Recopilación de la información a través del uso de los módulos auxiliares.
- Obtención de acceso mediante el uso de exploits y payloads.
- Escalación en los privilegios del sistema que se ataca.
- Ayuda a mantener la persistencia en el sistema víctima.
- Cubre las pistas del atacante, esto mediante módulos anti – forenses, que se usan después de que el ataque fue llevado a cabo.

Como se puede observar en los puntos anteriores, metasploit ofrece herramientas para cada una de las etapas que conforman un ataque, las cuales se vieron en el tema 3., adicionalmente, metasploit integra herramientas de seguridad, tales como NMAP, Nessus y Nexpose.

Beneficios que ofrece metasploit a los equipos de seguridad

Metasploit ofrece diferentes beneficios que ayudan a fortalecer las prácticas de ciberseguridad, dentro de las cuales se incluyen:

- **Simulación de escenarios:** los pentesters pueden realizar simulaciones de ataque y ver el sistema desde la perspectiva del atacante, esto les permite encontrar las vulnerabilidades del sistema, ayudándoles a mejorar la seguridad en el mismo, reparando las vulnerabilidades encontradas junto con otros vectores de ataque.
- **Automatización de tareas:** esta herramienta permite que los pentesters automaticen las tareas en los escenarios de prueba, ya que muchas partes del código se encuentran almacenadas en las bibliotecas antes mencionadas.
- **Optimización de casos de negocio:** proporciona informes de las vulnerabilidades que se deben de priorizar, con esto, los equipos de seguridad pueden tomar decisiones sobre la adquisición de nuevas herramientas de seguridad, las cuales pueden ayudar a mitigar los ataques.

Esta es una herramienta muy útil, la cual puede ser usada tanto para explotar vulnerabilidades como para corregirlas y brindar mayor protección, es una herramienta que es fácil de conseguir, incluso viene preinstalada en el sistema operativo Kali Linux.

(Belcic, 2020b; Ciberseguridad, s. f.-e; PCHARDWAREPRO, 2023; Platzi, 2019; Tech, s. f.)

3.4.2. Metodología OSSTMMv3

El Open Source Security Testing Methodology Manual o OSSTMM, en español conocido como Manual de Metodología de Pruebas de Seguridad de Código Abierto, es una estándar que sirve

para realizar pruebas de seguridad, debido a que es un estándar muy completo es muy común que sea usado para realizar auditorías de seguridad.

OSSTMM fue creado en el año 2001, por Pete Herzog, director ejecutivo del ISECOM (Institute for Security and Open Methodologies o Instituto de Seguridad y Metodologías Abiertas). Éste estándar considera que se cumplan las normas y buenas prácticas como las que establece el NIST (National Institute of Standards and Technology o Instituto Nacional de Estándares y Tecnología), la ISO (International Organization for Standardization u Organización Internacional de Normalización) e ITIL (Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologías de Información), solo por mencionar algunas, esto es lo que hace que éste estándar sea muy completo para la aplicación de pruebas de seguridad en las organizaciones.

El principal objetivo de OSSTMM es brindar un método científico para realizar pruebas sobre la seguridad de una organización, entre las cuales se encuentran las pruebas de penetración y el hacking ético, también provee guías para los auditores, las cuales están destinadas a las organizaciones para que puedan certificarse si cumplen con los requisitos establecidos por el ISECOM.

Con el paso del tiempo y el avance de la tecnología los sistemas se vuelven cada vez más complejos en comparación con años anteriores, ya que se agregan funcionalidades a los sistemas, como operaciones remotas, virtualización o computación en la nube, por lo que a su vez la infraestructura se vuelve más compleja, por esto mismo las pruebas de seguridad deben de realizarse de acuerdo a lo que el sistema ofrece.

OSSTMM se encuentra en constante evolución para adaptarse a estos nuevos cambios, para así aumentar su efectividad, por lo que la versión 3 de este estándar proporciona pruebas de seguridad operacional las cuales cubren cinco canales, con los cuales las organizaciones pueden comprender el alcance total de su seguridad, con esto también pueden determinar que tan bien funcionan sus procesos de seguridad, es decir, ven lo que realmente hacen sus operaciones de seguridad y no lo que suponen que deberían hacer. Los cinco canales son:

- **Seguridad humana:** la seguridad de la interacción y la comunicación humana se evalúan operativamente como medio de prueba.
- **Seguridad física:** está definida como cualquier elemento tangible de seguridad, por lo que se debe de evaluar.
- **Comunicaciones inalámbricas:** dentro de éstas se incluyen las comunicaciones electrónicas y señales, las cuales forman parte de la seguridad operativa.
- **Telecomunicaciones:** no importa si la red de telecomunicaciones es digital o análoga, cualquier tipo de comunicación realizada a través de la línea telefónica o de la red debe ser evaluada.

- **Redes de datos:** las pruebas que se realizan en este canal incluyen los sistemas electrónicos y redes de datos que se usan para la comunicación o interacción a través de cables y líneas de red cableadas.

Estos cinco canales son considerados como áreas operativas importantes, las cuales necesitan pruebas de seguridad adecuadas para que la organización esté protegida correctamente.

El esquema general del proceso que deben seguir las pruebas de seguridad tiene las siguientes fases:

- **Fase de inducción:** el analista debe de comprender los requerimientos de la auditoría, así como su alcance y sus limitaciones. Después de esta fase se determina el tipo de prueba que debe hacerse. Esta fase tiene tres módulos:
    - Revisión de la postura.
    - Logística.
    - Verificación de detección activa.

- **Fase de interacción:** se necesita conocer cuál es el alcance en relación a los objetivos. Es en esta fase donde se define el alcance. Los módulos de esta fase son:
    - Auditoría de visibilidad.
    - Verificación de acceso.
    - Verificación de confianza.
    - Verificación de controles.

- **Fase de investigación:** el auditor descubre información, donde verifica que la administración se lleve a cabo de acuerdo a lo planeado. Esta fase tiene los siguientes módulos:
    - Verificación del proceso.
    - Verificación de configuración.
    - Validación de propiedad.
    - Revisión de segregación.
    - Verificación de exposición.
    - Inteligencia competitiva.

- **Fase de intervención:** se centra en los recursos que requieren los objetivos, estos se pueden conmutar, cambiar, sobrecargar o privar, con el objetivo de provocar penetración o interrupción. Regularmente es la última fase de las pruebas de seguridad. Los módulos de esta fase son:
    - Verificación de cuarentena.
    - Auditoría de privilegios.
    - Continuidad del servicio.
    - Revisión de alertas y registros.

Estos módulos pueden observarse en la figura 3.14. La combinación de todos los módulos da como resultado una metodología aplicable a todos los tipos de pruebas de seguridad, sin importar si es un sistema en particular, un solo proceso o varios procesos, ya que esta metodología garantiza que las pruebas realizadas son completas y eficientes.

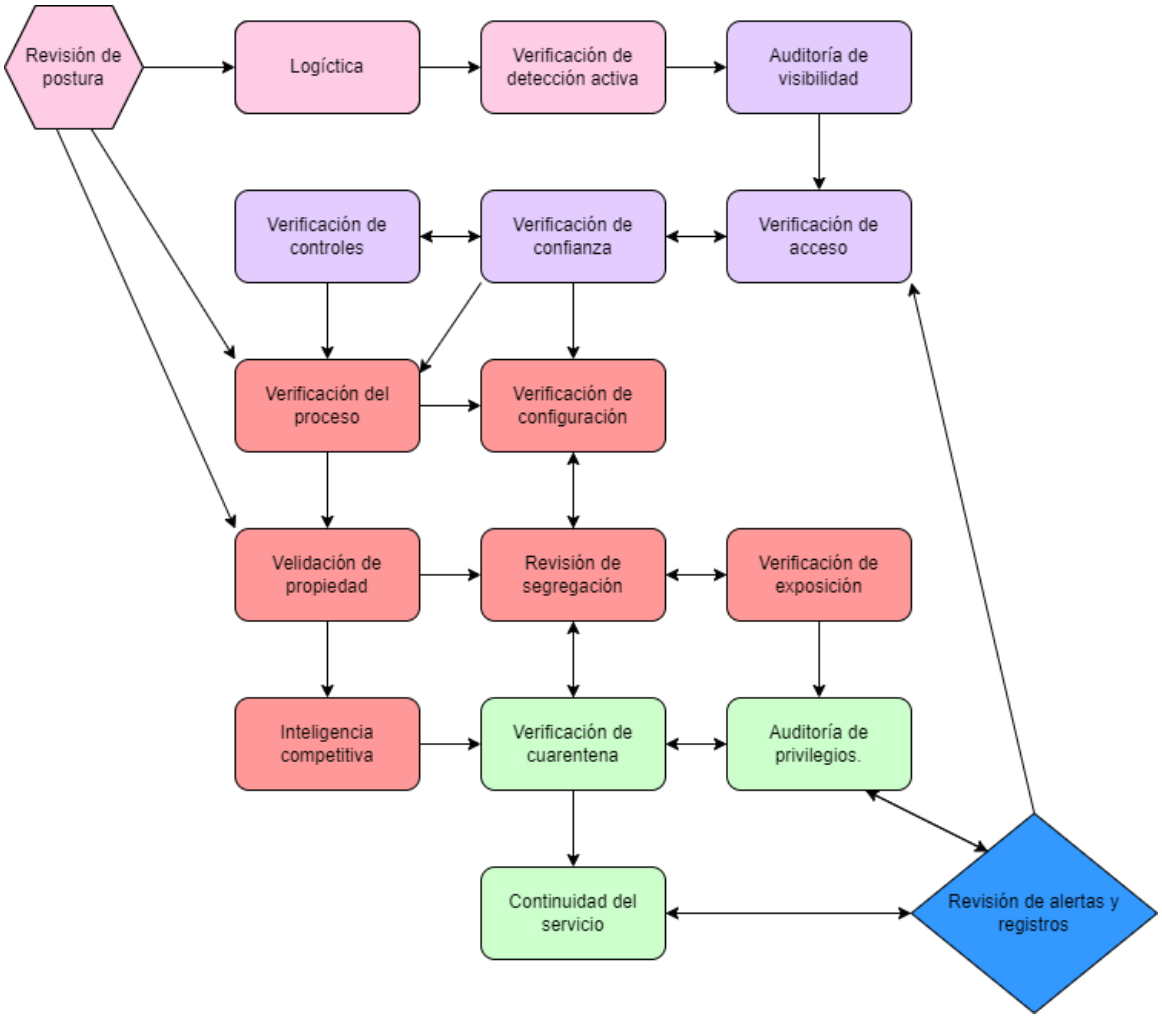


Figura 3.14. Esquema general de las pruebas de seguridad.

Herzog, P. & ISECOM. (s. f.).

(Ciberseguridad, s. f.-f; DragonJAR, 2010; GlobátiKa, 2019; ISECOM, s. f.; Junta de Andalucia, s. f.-a)

3.4.3. Pentesting

El término *pentesting* proviene de las palabras *penetration* y *test.* Este puede ser definido como un conjunto de metodologías y técnicas usadas para descubrir vulnerabilidades y/o fallos de seguridad en un sistema, para corregirlos de forma eficaz. En otras palabras, es una simulación de ataque autorizado contra un sistema, este tiene como propósito evaluar la seguridad del mismo, y con los resultados, el pentester puede realizar una evaluación de los riesgos, esto es muy importante para las organizaciones, ya que pueden identificar que tan seguro es su sistema si llegara a ser atacado.

Tipos de pentesting

Los tipos de pentesting se dividen en dos:

1. **Origen de las pruebas:** estas se clasifican de acuerdo con el rol que desarrolla el pentester al realizar las pruebas de penetración:

    a. **Auditoría externa o cover pentest:** el pentester asume ser un atacante externo, que sin haber hecho previamente una investigación de la organización puede obtener información sensible que ponga en riesgo la privacidad de dicha organización, al realizar esto se están poniendo a prueba las barreras de seguridad que se tienen implementadas entre el internet y la red corporativa. Algunas de las actividades realizadas en este tipo de auditorías son:
        i. Barrido de líneas telefónicas.
        ii. Evaluación de la seguridad en las centrales telefónicas.
        iii. Análisis a sistemas con acceso remoto.
        iv. Situación de la seguridad en la conexión a internet.
        v. Seguridad en la conexión con otras redes.
        vi. Seguridad de aplicaciones web.
        vii. Seguridad en redes inalámbricas.

    b. **Auditoría interna u overt pentest:** este tipo de auditoría tiene como objetivo evaluar la seguridad en el entorno privado de la organización, por lo que el pentester tiene el rol de un atacante que puede acceder a la red interna de la organización. Las principales actividades que se realizan en estas auditorías son:
        i. Pruebas de nivel de seguridad en los dispositivos de red internos.
        ii. Pruebas de seguridad en los principales servidores.
        iii. Pruebas de seguridad de las estaciones de trabajo.
        iv. Seguridad de las aplicaciones.

2. **Conocimiento del objetivo:** cuando ya se tiene fijado el objetivo de ataque se pueden realizar tres tipos de pruebas para investigar las posibles vulnerabilidades del sistema:

a. **Caja blanca:** esta es una de las pruebas más completas, parten de un interés general. Para realizar este tipo de pentesting, la organización le debe de proporcionar al pentester la mayor información posible, como: la cantidad de equipos que componen la red, los tipos de sistemas, la estructura de la red, servidores, contraseñas, documentación, entre otra información. El pentester con toda esta información puede detectar los puntos de falla y vulnerabilidades potenciales.

   Este tipo de prueba se centra en los procesos del sistema y en el software, se puede hacer uso de hardware de búsqueda para encontrar errores en el código fuente de las aplicaciones o malas configuraciones en software y hardware. Las pruebas de caja blanca arrojan resultados más precisos, además detecta amenazas de forma inmediata y defectos en las configuraciones y construcciones. En las pruebas de caja blanca no se logra hacer la simulación del ataque.

b. **Caja negra:** para realizar este tipo de prueba, el pentester no cuenta con la información brindada por la organización como con de las pruebas de caja blanca. Esta prueba es algo más cercana a la realidad de lo que se encontraría el atacante, pues les muestra a las organizaciones que tan fuerte es la seguridad con la que cuentan, ya que el pentester realiza una simulación de ataque sobre el sistema, proporcionándole a las organizaciones una estimación real de las amenazas e información que obtiene, con solo tener acceso a la información pública.

   Un inconveniente de estas pruebas es que para que el pentester realice la evaluación tendría que hacer mucho esfuerzo, por lo que podrían pasar desapercibidas puertas traseras o vulnerabilidades parciales, por lo que se brindarían recomendaciones muy generales.

c. **Caja gris:** son una mezcla de las pruebas de caja blanca y negra. El pentester simula ser un usuario con privilegios, por lo que tiene cierta información con la cual puede realizar las pruebas.

   Las pruebas de caja gris se suelen usar cuando se quieren identificar vulnerabilidades en solo ciertos sectores, son más reales, además proporcionan una estimación más real de las amenazas y vulnerabilidades que pudiera tener la organización.

El tipo de pentesting elegido se puede elegir teniendo como base las condiciones de la organización, ya que esto depende del tipo de información que se tenga y también del sistema sobre el cual se quiera aplicar.

Con estas pruebas, la organización puede determinar las posibilidades de éxito de un ataque, asimismo se identifican los fallos de seguridad y pueden implementar medidas para mitigar el riesgo de ataque.

Fases del pentesting

El pentesting se conforma de cuatro etapas:

1. **Reconocimiento:** en esta etapa se definen los objetivos de la prueba, el entorno e información adicional necesaria para simular el escenario de ataque. También en esta etapa se aprovecha para recopilar toda la información posible de la organización, como dispositivos de red, servidores, estaciones de trabajo, software que se utiliza, entre otros, esto con el fin de comprender el funcionamiento de la organización y conocer sus potenciales debilidades.
   Si un atacante es quien recolecta la información puede hacerlo de forma pasiva o activa (tema 3.1.2). Si el pentesting se está haciendo legalmente, se debe definir un acuerdo de nivel de servicio o algún otro documento que muestre evidencia de que la organización dio autorización para realizar el pentesting.
2. **Búsqueda de vulnerabilidades:** en esta fase se hace un análisis de la información que se recolectó en la fase de reconocimiento, con el propósito de buscar vulnerabilidades en el sistema. Para esta búsqueda se pueden utilizar diferentes herramientas, como NMAP, Nessus, OpenVas o Nexpose. En algunos casos, las pruebas de pentesting pueden terminar en esta fase, ya que al encontrar las vulnerabilidades de la organización se han alcanzado los objetivos establecidos.
3. **Explotación de vulnerabilidades:** en esta etapa se explota una de las vulnerabilidades encontradas en la etapa anterior, esto con el fin de intentar comprometer el sistema o la aplicación atacada. El objetivo de esta etapa es tomar el control del sistema y escalar el nivel de privilegios, para después acceder a información más importante. Un atacante en esta fase puede ocupar toda la información que ha obtenido para mantener el acceso al sistema o también para generar nuevos accesos por si se requiere acceder en el futuro.
4. **Generación de informes:** finalmente, el pentester debe realizar la documentación de todo lo que realizó, este informe incluye: técnicas utilizadas, información relevante encontrada, herramientas usadas, las vulnerabilidades que se encontraron, y demás cosas que le permitan a la organización saber el nivel de seguridad con el que cuentan, y lo que deben corregir. Adicionalmente, se entrega un análisis de los riesgos y las recomendaciones de seguridad. Se entrega un informe técnico, el cual está dirigido al personal de TI y un informe general, el cual es más específico e incluye estadísticas del número de vulnerabilidades encontradas, la cantidad de equipos comprometidos, facilidad de explotación, entre otros.

Las pruebas de pentesting son muy útiles para que una organización descubra las vulnerabilidades que tienen y las corrija antes de que un atacante se aproveche de ellas, ocasionándoles pérdidas.

(E. Fernández, 2019b; Ginzo, 2021; INCIBE, 2019a; Romero Vanegas, s. f.)

3.4.4. Manejo de exploits y análisis de vulnerabilidades en la red

3.4.4.1. Exploits

Un exploit es un programa que se aprovecha de las vulnerabilidades de un sistema para obtener información confidencial, la cual un atacante podría usar en su beneficio. Los exploits son un riesgo permanente, pues la seguridad que implementan las organizaciones debe de ser muy eficiente para evitar que un exploit pueda comprometer su información confidencial.

Hay diferentes tipos de exploits:

- **Exploits remotos:** son los exploits que tienen como objetivo un dispositivo conectado a una red diferente a la que el atacante está conectado, para hacer uso de exploits de este tipo, el atacante debe aprovecharse de un fallo externo en la red objetivo para que así pueda acceder al dispositivo víctima.
- **Exploits locales:** para usar este tipo de exploits, el atacante debe estar conectado a la misma red a la cual está conectado el dispositivo víctima, y para acceder a dicho dispositivo, el atacante deberá aprovecharse de un fallo de seguridad que haya en el dispositivo víctima.
- **Exploit cliente:** son los más comunes, para que se puedan ejecutar, el usuario del sistema víctima necesita realizar una acción, como descargar un archivo o acceder a un enlace.
- **Exploits conocidos:** son los exploits que ya se sabe públicamente que vulnerabilidad afectan, por lo que se pueden tomar medidas de seguridad para corregir estas vulnerabilidades lo antes posible, estas pueden corregirse mediante la instalación de parches de seguridad o actualizaciones del software.
- **Exploits de día cero:** este tipo de exploits se crean inmediatamente después de que el atacante descubre la vulnerabilidad, se llaman de día cero porque el ataque a la vulnerabilidad sucede el mismo día que la vulnerabilidad fue descubierta. Este tipo de exploits son muy peligrosos porque no se tiene una solución inmediata.

El entorno de trabajo que usan los exploits son los frameworks, el más conocido es Metasploit (tema 3.4.2), esta herramienta es comúnmente usada en la fase de explotación de vulnerabilidades durante el proceso de pentesting (tema 3.4.3).

Para proteger el sistema de ataques de exploit se pueden seguir las siguientes recomendaciones:

- **Mantener el software actualizado:** permitir las actualizaciones automáticas si el dispositivo lo permite, en caso contrario, estar pendiente de las actualizaciones para poder instalarlas lo antes posible.
- **Hacer copias de seguridad:** esto es muy útil cuando se tiene un exploit de día cero, ya que al ser una vulnerabilidad recientemente descubierta no se puede hacer mucho para solucionarla inmediatamente, por lo que realizar copias de seguridad de la información almacenada es importante, para evitar pérdidas.
- **Software de confianza:** se tiene que usar software de proveedores de confianza, ya que los desarrolladores se aseguran de que sus productos sean a prueba de exploits, y si llegara a haber un exploit de día cero harían todo por solucionarlo en la menor cantidad de tiempo posible.

(Ayudaley, 2021; Grupo Atico34, 2021a)

3.4.4.2. Análisis de vulnerabilidades

Un análisis de vulnerabilidades es un proceso que identifica las vulnerabilidades de un sistema, fallas, brechas de seguridad, puntos de acceso inseguros, errores de configuración, entre otros, y les asigna una prioridad de acuerdo al riesgo que representan.

Realizar el análisis de vulnerabilidades tiene una gran importancia, porque si una vulnerabilidad es explotada, la organización víctima puede tener pérdidas económicas o de datos, lo que afecta directamente su reputación, por lo que al realizar un análisis de este tipo se puede establecer un entorno seguro y también se puede decidir la mejor manera de mitigarlas, sin embargo, realizar estos análisis de forma manual en todos los dispositivos del sistema resulta sumamente complicado, para ello existen herramientas de análisis de vulnerabilidades, estas ejecutan los análisis de manera automática y muestran una lista del software usado junto con sus vulnerabilidades, con esto las organizaciones pueden tomar acciones para evitar que un atacante explote alguna de vulnerabilidad.

Tipos de análisis de vulnerabilidades

- **Análisis no autenticado:** no requiere algún tipo de autenticación en el sistema para realizar el análisis, por lo que los resultados no son concluyentes, este tipo de análisis

solo recopila las vulnerabilidades que se pueden detectar desde un punto de vista externo.

- **Análisis autenticado:** para realizar este tipo de análisis se requiere iniciar sesión en el sistema, este análisis proporciona resultados concluyentes ya que es realizado desde el punto de vista de un usuario confiable.
- **Análisis externos:** son los que se realizan en los sistemas expuestos a internet. Las vulnerabilidades se identifican desde afuera, es decir, se valida si se puede realizar una conexión interna a la organización y escalar privilegios, obtener información sensible o visualizar las bases de datos.
- **Análisis interior:** son los análisis que se realizan internamente en la organización, en estos se valida hasta dónde puede llegar un usuario en el sistema con los privilegios que tiene asignados, asimismo verifica si la información viaja de manera segura.
- **Análisis no intrusivos:** estos solo detectan las vulnerabilidades y las reportan para que puedan solucionarse.
- **Análisis intrusivos:** estos después de detectar las vulnerabilidades intentan explotarlas, estos son útiles para estimar el riesgo de impacto que causa dicha vulnerabilidad, pero como desventaja es que afectan las operaciones de la organización.

Metodología del análisis de vulnerabilidades

1. **Acuerdo de confidencialidad:** para realizar el análisis de vulnerabilidades debe de existir un acuerdo de confidencialidad entre la organización y el analista, esto porque durante el proceso de análisis, el analista puede acceder a información confidencial de la organización, y debe existir un acuerdo en donde se indique la información encontrada solo será usada con fines informativos.
   También, la organización debe confiar en el analista y proporcionarle toda la información que necesite, dependiendo del tipo de análisis que realizará.
2. **Determinar las "reglas del juego":** deben de establecerse los límites, permisos y obligaciones que deben de tener en cuenta todas las partes involucradas. Al realizar un análisis de vulnerabilidades el sistema debe de estar trabajando de forma regular, por lo que los usuarios no deberían ser avisados, esto para que sigan usando el sistema como lo hacen regularmente, ya que si se les avisa pueden cambiar algunos comportamientos al usar la red, y el análisis no tendría el mismo efecto.
3. **Recogida de información:** el propósito de un análisis de vulnerabilidades es recopilar información, por lo que se pueden realizar pruebas de caja blanca, negra o gris.
   Deben realizarse diferentes tipos de análisis de vulnerabilidades, para tener una mayor certeza de que el análisis realizado es lo más completo posible, entre algunos de los tipos de análisis que se pueden elegir se encuentran:
   a. **Análisis interior:** para mostrar hasta dónde puede llegar un usuario con los privilegios que se le fueron asignados, este análisis debe realizarse con las credenciales de acceso de un usuario del sistema.

   b. **Análisis exterior:** el objetivo de este tipo de análisis es acceder remotamente a los servidores de la organización, y tratar de conseguir privilegios que solo deberían tener usuarios autorizados.
4. **Documentación e informes:** después de haber realizado el análisis de vulnerabilidades, el analista debe presentar un informe detallado de todo lo que realizó y cuáles son los resultados que obtuvo, también se debe incluir una lista de las vulnerabilidades detectadas, una lista donde se indiquen los dispositivos y servicios vulnerables y el nivel de riesgo de las vulnerabilidades encontradas en cada servicio y dispositivo analizado.

Después de que la organización tiene el informe del análisis de vulnerabilidades debe de comenzar a trabajar en repararlas para reducir el riesgo de que sean explotadas, para esto puede instalar parches de seguridad y realizar los cambios necesarios en la configuración.

La desventaja que tiene el proceso de parcheo y configuración es que pueden poner en riesgo todo el sistema, por lo que es recomendable que las configuraciones y parches se instalen en un solo dispositivo para hacer pruebas y verificar si hay o no problemas.

Después de que se hicieron las pruebas necesarias y que se tenga la certeza de que no se ocasionarán problemas se pueden aplicar los parches y configuraciones a los demás dispositivos.

(Ciberseguridad, s. f.-a; Romero Castro et al., 2018)

3.4.5. Promiscuidad en redes

El modo promiscuo es un estado en el que las tarjetas de red (Network Interface Card o NIC) pueden ser configuradas para que puedan capturar todo el tráfico que pasa por ellas.

Una NIC “escucha” el encabezado de los paquetes que pasan por la red a la que está conectada, su funcionamiento normal es solo aceptar y procesar los paquetes que van dirigidos a ella. Las direcciones de destino de los paquetes que viajan en la red pueden ser unicast, multicast o broadcast.

Una dirección de destino unicast hace referencia a un único dispositivo de destino, es decir, solo un dispositivo de la red puede aceptar y procesar el paquete. Una dirección de destino multicast hace referencia a un grupo de dispositivos de la red que puede aceptar y procesar el paquete, mientras que una dirección de broadcast se refiere a que todos los dispositivos del dominio de broadcast en cuestión podrán recibir y procesar el paquete.

Cuando una NIC es configurada para trabajar en modo promiscuo, capturará todo el tráfico que circula por la red a la que está conectada, sin importar cual sea su dirección de destino, después de haberlo capturado creará una copia del paquete y lo enviará de nuevo por la red para que

llegue a su verdadero destino. El funcionamiento del modo promiscuo es muy similar al funcionamiento de los sniffers, ya que estos capturan todo el tráfico de la red a la cual se conectan.

Los analizadores de redes, analizadores de protocolos y rastreadores de paquetes también usan el modo promiscuo para inspeccionar el tráfico que circula por la red, por lo que, usar este modo puede ser peligroso y útil a la vez, todo depende de las intenciones de quien lo use, por ejemplo, un administrador de sistemas puede usar el modo promiscuo para diagnosticar problemas en la red, mientras que un atacante puede usarlo para espiar los datos que circulan por la red y conseguir información importante.

(Ramírez González, s. f.; Spiegato, 2021a)

3.4.6. Robo de identidad

El robo de identidad es un delito donde el atacante se apropia de la identidad de otra persona para asumir su identidad, puede robar información personal de su víctima como contraseñas, números de tarjetas, datos de seguridad social, entre otros, para realizar algún tipo de fraude.

El robo de identidad puede ser desde hackear una cuenta de red social, hasta realizar compras o préstamos a nombre de la víctima. En los últimos años ha habido un incremento de este tipo de delito debido a que las personas publican mucha información de sí mismos en internet, al hacer esto, su información queda expuesta a prácticamente todas las personas.

Después de que el ladrón robó la identidad de su víctima puede convertirlo en fraude de identidad, este se da cuando el ladrón hace uso de la información de su víctima para hacerse pasar por ella y realizar acciones en su nombre, dichas acciones afectan a la víctima de tal forma que pueden pasar muchos meses o incluso años intentando resolver el delito, sin tener garantía que se recuperará totalmente de sus pérdidas.

Métodos de robo de identidad

Los métodos más comunes para realizar el robo de identidad pueden clasificarse en los siguientes tres tipos:

- **Sin acceso a internet:** en este método de robo de identidad, ni la víctima ni el estafador necesitan acceder a internet, solo basta que el ladrón use sus habilidades para aprovechar los descuidos de la víctima y usarlos en su beneficio.
    - **Ingeniería social:** como se mencionó en el tema 3.2.5, es una técnica que se basa en la interacción social, a través de conversaciones con la víctima, el ladrón obtiene la información que necesita mediante la manipulación y el engaño.
    - **Shoulder surfing:** esta técnica usa el espionaje de forma muy cercana para obtener información, el ladrón observa a espaldas de la víctima las teclas que

digita, el monitor u otro dispositivo que sea de su interés y que le de información, esta es una técnica muy usada para conseguir usuarios, contraseñas, códigos de seguridad, entre otros.
    - **Eavesdropping:** esta técnica consiste en recolectar información escuchando conversaciones privadas.
    - **Dumpster Diving:** consiste en buscar información en la basura de las organizaciones, tema 3.2.6.
- **Sin acceso a internet, usando herramientas tecnológicas:** en este método se usan técnicas que no requieren tener acceso a internet, sin embargo, estas técnicas hacen uso de herramientas electrónicas:
    - **Clonación de tarjetas:** la clonación de tarjetas consiste en hacer una copia de la tarjeta de la víctima sin su consentimiento, para realizar esto, los delincuentes usan dispositivos electrónicos programados que sirven para guardar los datos que contiene la tarjeta en la cinta magnética, para después poder clonar esa información a otro plástico.
    - **Vishing y smishing:** estas técnicas son un tipo de phishing, visto en el tema 3.1.2.

- **Con acceso a internet:** este método requiere que la víctima use alguna aplicación en internet.
    - **Spam:** puede considerarse spam a cualquier correo electrónico que fue recibido por destinatarios que no solicitaron dicho correo. Un mensaje de spam tiene que cumplir ciertas características:
        - Ser enviado de forma masiva.
        - Ser un mensaje no solicitado por el usuario.
        - Tener contenido engañoso.

      Si un usuario recibe un mensaje de spam e interactúa con el contenido engañoso que el atacante le ha enviado es cuando comienza a ser víctima del robo de información, la cual posteriormente el atacante puede usar para su beneficio.
    - **Keylogger:** registra las pulsaciones del teclado de la víctima, y envía toda la información captada al atacante (tema 3.2.4).
    - **Suplantación de identidad:** el atacante se hace pasar por una entidad legitima y de confianza para que la víctima proporcione toda la información que le piden, las víctimas suelen caer en este tipo de engaños porque el atacante tiende a usar imágenes de Copyright de sitios legítimos, por lo que a simple vista podría parecer un sitio de confianza, sin embargo, hay que estar atento a los detalles, para evitar caer en este tipo de engaños.

Detección, protección y prevención de robo de identidad

El robo de identidad es muy frecuente, sin embargo, hay grupos en la población que son más susceptibles:

- **Personas mayores:** para los ladrones son un blanco fácil porque puede ser que estas personas no estén muy relacionadas con la tecnología, por lo que podrían caer muy fácilmente en engaños por parte de los delincuentes, además, las víctimas de este grupo tienen menos habilidades con la tecnología, por lo que es difícil para ellos detectar las amenazas que circulan por la red.
- **Personas con ingresos altos y dueños de empresas:** el blanco perfecto de los atacantes son personas con títulos importantes e ingresos elevados, esto porque pueden obtener un mayor beneficio.
- **Militares destinados en el extranjero y presos:** estos grupos de personas no pueden hacer un seguimiento periódico de sus finanzas, por lo que un ladrón podría robar su identidad y no podrían percatarse a tiempo. De igual forma, los amigos y familiares de este grupo pueden aprovecharse de la falta de control sobre sus finanzas para realizar actividades mal intencionadas sin ser descubiertos.
- **Ghosting:** este término hace referencia al robo de identidad de una persona fallecida, si nadie lo nota, un ladrón puede hacerse pasar por la persona muchos años sin ser descubierto.

Hay que estar pendientes para detectar actividad sospechosa que sea indicio del robo de identidad. Hay que consultar frecuentemente estados de cuenta, facturas, historiales crediticios, entre otros para detectar si hay actividad no reconocida y en caso de ser así hacer los reportes correspondientes para evitar que el ladrón se siga aprovechando, además hay que bloquear las cuentas afectadas, para que así el ladrón ya no pueda usarlas.

También hay que poner atención en inicios de sesión no reconocidos, actualmente muchas de las aplicaciones mandan notificaciones que indican que se ha accedido a la cuenta desde un dispositivo no reconocido, esto es una señal de alarma que por nada debe dejarse pasar, ya que es un claro indicio que otra persona cuenta con las credenciales de acceso, de ser posible hay que habilitar la verificación en dos pasos, para tener una capa más de seguridad.

De igual manera, si se reciben llamadas, mensajes o correos electrónicos donde soliciten información, antes de proporcionarla hay que asegurarse que el remitente sea quien dice ser, en dado caso de que se tenga que acceder a algún sitio web, hay que cerciorarse que dicho sitio sea de legítimo antes de introducir información importante.

También hay que estar atento a lo que se descarga, solo hay que hacerlo de fuentes confiables para evitar descargar un malware que pueda espiar la actividad que se realiza en el dispositivo.

Un error bastante común es publicar mucha información personal en redes sociales, esto le da herramientas a los ladrones para robar información más fácilmente, ya que muchas personas suelen usar contraseñas que involucran su nombre, fecha de nacimiento, el nombre de algún familiar, mascota, entre otros, lo recomendable es usar una contraseña que mezcle mayúsculas, minúsculas, números y símbolos para hacerla más segura, aunado a esto se tiene que es un

error anotar contraseñas y dejarlas visibles ya que es una manera muy fácil que alguien tenga acceso a ellas.

Como se puede observar, mantenerse seguro en la red es una tarea complicada, por lo que hay que seguir las anteriores y más recomendaciones de seguridad para evitar ser víctimas de robo de identidad.

(Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, s. f.; Federal Trade Comission Consumer Advice, 2021; INAI, s. f.-a; USAGov, 2023)

3.4.7. Engaño a firewalls y detectores de intrusos

3.4.7.1. Engaño a firewalls

Los firewalls son elementos que monitorean el tráfico que entra y sale de la red (tema 3.3.4). Las reglas de filtrado que ocupa un firewall se basan en examinar de la cabecera de los paquetes los campos siguientes:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de origen.
- Puerto de destino.

Con base en los valores que examina es como decide si permite o deniega el paso del tráfico en la red. Una forma que un atacante puede usar para engañar a un firewall e infiltrarse en la red es modificar la dirección IP del dispositivo con el que llevará a cabo el ataque, esto para que coincida con alguna de las direcciones IP que el firewall tiene permitido dejar pasar. Este método tiene como desventaja que se puede tener un conflicto de direcciones IP, es decir, puede ser que haya dos dispositivos en la red que tengan la misma IP, lo que causaría un conflicto en la comunicación.

Una alternativa para lograr engañar a un firewall es usar ARP spoofing, esta es una técnica usada por los atacantes para lograr entrar a una red y robar, detener o modificar los datos que pasan por la misma. Al usar ARP spoofing, el atacante envía mensajes ARP falsos, con los que puede vincular la dirección MAC del dispositivo atacante, con una dirección IP que el firewall tenga permitido dejar pasar.

Otra técnica que sirve para evitar un firewall es NAT Slipstreaming, esta técnica permite acceder de manera remota a los servicios TCP/UDP en el equipo de la víctima, saltándose los sistemas NAT/Firewall, aprovechándose de ALG (Application Layer Gateway o Puerta de enlace de capa de aplicación).

ALG es un componente de software diseñado para administrar protocolos específicos, como SIP (Session Initiation Protocol o Protocolo de inicialización de sesión) o FTP, este actúa como intermediario entre internet y un servidor de aplicaciones. ALG actúa como servidor de punto final y controla si se debe permitir o denegar el tráfico al servidor de aplicación.

Lo que permite ALG es que las aplicaciones cliente usen puertos TCP/UDP dinámicos para que se puedan comunicar con los puertos que usa el servidor para ofertar sus servicios. Si se careciera de un ALG, los puertos del servidor serían bloqueados, el administrador del sistema tendría que abrir varios puertos, lo que provocaría un debilitamiento en la red, por lo que el sistema podría ser atacado por alguno de esos puertos.

Para llevar a cabo NAT Slipstreaming, el atacante envía a la víctima un enlace malicioso, cuando la víctima accede a dicho link se activa el gateway lo que permite abrir cualquier puerto TCP/UDP de la víctima, lo que permitiría que el perpetrador realice un ataque a dicho sistema.

Después surgió una variante de NAT Slipstreaming, en la cual el atacante puede crear conexiones con cualquier dispositivo de la red, y no solamente con el dispositivo que visitó el link malicioso.

Este ataque se está previniendo desde el punto de vista de los navegadores, por lo que una medida de seguridad para evitar ser atacando usando esta técnica es usar versiones actualizadas del navegador y evitar el uso de navegadores en entornos de producción o aquellos que ya dejaron de tener soporte.

(Cyberseguridad.net, 2021; Jiménez Jiménez, s. f.)

3.4.7.2. Engaño a IDS

Un IDS es un elemento de seguridad que se encarga de monitorear el tráfico que circula por un sistema. Su propósito es identificar los intentos de ataque o amenazas que comprometen la seguridad del sistema.

Dependiendo de su función, los IDS es que se clasifican de la siguiente manera:

- **En función de los sistemas que vigilan:** se enfoca en los sistemas que analizan la actividad de un host o los que analizan una red en busca de posibles ataques. Dentro de esta clasificación se incluyen:
    - **IDS basados en red:** monitorea los datos que se transmiten en la red, para encontrar elementos que caractericen una posible amenaza. Este tipo de IDS usa un sniffer para capturar y analizar los datos que circulan por la red, con el objetivo de buscar patrones que sean indicios de algún tipo de ataque. El análisis realizado es en tiempo real, por lo que además trabajar a nivel TCP/IP y capa de transporte también trabaja en la capa de aplicación. Este IDS puede instalarse en alguno de

los hosts de la red o en alguno de los elementos que analiza el tráfico, como un router.
    - **IDS basados en host:** monitorea el tráfico entrante y saliente de un host en específico, solo actúa en ese host. Este tipo de IDS es recomendable para servidores web

- **En función de cómo realizan su desempeño:** esta clasificación hace referencia a la forma en cómo es que realizan la detección de ataques. Esta categoría se subdivide en:
    - **Detección de anomalías:** estos suponen que la intrusión se puede ver como una anomalía, esto se debe a que un IDS sabe cuál es el comportamiento habitual del sistema, por lo que al notar cambios en el comportamiento podría detectar una amenaza basándose en tales cambios. En este se definen los patrones de ataque conocidos sin sus posibles variaciones.
    - **Detección de usos indebidos:** este indica que pueden definirse patrones para los ataques conocidos y para sus posibles variaciones, por lo que analizaría el sistema buscando variaciones en su comportamiento.

3.4.7.3. Evasión de IDS

Existen diferentes vectores de ataque que permiten evadir un sistema IDS:

- **Ataque DoS:** muchas veces el IDS tiene asignada una IP, si el atacante llega a conocer dicha IP puede crear un ataque de denegación de servicios, al realizar esto, el atacante satura de información el IDS, por lo que dejaría pasar el exceso de información de manera libre. El objetivo de esta técnica es hacer que colapse el IDS para que el atacante pueda entrar a la red.
- **Generador de falsos positivos:** si el atacante tiene información suficiente sobre el IDS puede manipular los paquetes de datos para que generen falsos positivos en sus detecciones, al hacer esto de manera repetida, el IDS tendrá dificultades para diferenciar los falsos positivos de los ataques reales.
- **Fragmentación:** el IDS tiene un tiempo de espera de 15 segundos para reensamblar los paquetes y el host victima tiene un tiempo de espera de 30 segundos, para hacer este tipo de evasión, el atacante envía el primer fragmento del paquete, por lo que el IDS y la víctima lo reciben, después el IDS se queda esperando por 15 segundos el segundo fragmento que completa el paquete, el atacante debe esperar esos 15 segundos sin enviar nada, por lo que el IDS al no recibir la segunda parte del paquete descarta la primera parte, después de que la descarta, el atacante ahora si envía la segunda parte del paquete y el IDS lo recibe pero no puede reensamblarlo con nada porque descartó la primer parte, pero el host victima sigue esperando ya que tiene un tiempo de espera superior para el reensamblado, por lo que recibe el paquete de datos malicioso sin que haya sido detectado por el IDS.

- **Flooding:** en este método, el atacante envía una gran cantidad de tráfico para provocar lentitud en el proceso de análisis del IDS, por lo que, si el IDS no analiza el tráfico adecuadamente, podría dejar pasar conexiones maliciosas.
- **Cifrado:** si el atacante consigue cifrar la conexión entre el host víctima y la máquina del atacante, el IDS no podrá reconocer patrones de ataque, ya que, al estar todo cifrado, ningún elemento intermediario podrá entender la información que circula por ambos dispositivos.

(Ávila, 2018; Jiménez Jiménez, s. f.; J. Moreno, 2010)

3.4.8. Vulnerabilidades en el software

Las vulnerabilidades de software son uno de los principales problemas a los que se enfrentan los departamentos de seguridad de las organizaciones, estas son fallas en la seguridad de una aplicación, con las cuales un atacante compromete la seguridad del sistema sobre el que se ejecuta dicha aplicación. De manera general, todos los softwares tienen vulnerabilidades, y su gravedad depende de si son usadas o no para dañar el sistema.

Una vulnerabilidad en un software puede ser un error en el código o en su configuración, esto no significa que todos los errores de programación se convierten en fallas de seguridad, los errores de programación pueden causar que un programa no funcione de la manera que se espera, sin que esto ponga en riesgo la seguridad del sistema.

Las vulnerabilidades están definidas por cinco parámetros:

- **Producto:** para definir una vulnerabilidad hay que saber a qué productos afecta, es decir, la vulnerabilidad puede afectar solo a una versión del software, a un grupo de programas diferentes pero que compartan el mismo fallo, esto pasa cuando la vulnerabilidad reside en sistemas operativos diferentes, por ejemplo, si hay una vulnerabilidad en el kernel de Linux, todas las distribuciones que usen dicho kernel se verán afectadas.
- **Donde:** hay que identificar en que parte del software se encuentra la vulnerabilidad, regularmente los programas se componen de módulos, por lo que habría que identificar en que modulo se encuentra la vulnerabilidad, es posible que si dicho módulo no está activo la vulnerabilidad no se pueda explotar.
- **Causa y consecuencia:** la causa es el error que cometió el programador y la consecuencia son los riesgos que trae consigo dicho error, por ejemplo, si el programador no puso límites para el valor de una variable como consecuencia podría tenerse un desbordamiento de memoria.
- **Impacto:** esto es lo que el atacante puede conseguir si se aprovecha de la vulnerabilidad. El impacto sirve para definir la gravedad de la vulnerabilidad.

- **Vector de ataque:** esto hace referencia a como un atacante aprovecha las vulnerabilidades. Un vector de ataque común es cuando se envía información manipulada a un puerto en concreto del sistema, otro vector de ataque es cuando el atacante hace que la víctima visite un sitio malicioso.

Para gestionar las vulnerabilidades, el MITRE (MITRE Corporation), una organización estadounidense sin fines de lucro que apoya a agencias gubernamentales de seguridad en EE.UU, creó un sistema para estandarizar las vulnerabilidades y conocer su gravedad. Este sistema se compone de CVE (Common Vulnerabilities and Exposures, o en español Vulnerabilidades y Exposiciones Comunes), CVSS (Common Vulnerabilities Scoring System o Sistema Común de Calificación de los Puntos Vulnerables por su traducción al español) y CVRF (Common Vulnerability Reporting Framework o Informes de Vulnerabilidad Común).

El CVE se encarga de identificar unívocamente las vulnerabilidades mediante un código, el formato de este código es el siguiente:

- CVE – año de asignación – número 4 dígitos
    - El identificador comienza con CVE, seguido del año en el que se asignó el código a la vulnerabilidad, seguido de un código de cuatro cifras

El CVE ha sido aceptado ampliamente, porque es muy difícil identificar una vulnerabilidad solo por sus características, ya que muchas son parecidas entre sí, o se tiene muy poca información de ellas, por lo que la manera más fácil de identificarlas es por su CVE.

El CVSS es el puntaje que identifica la gravedad de una vulnerabilidad de software, esto permite dar prioridad al momento de crear los parches de seguridad. Clasifica el impacto al aprovechar el fallo de seguridad teniendo en cuenta la triada CID y demás datos que se puedan obtener aprovechando la vulnerabilidad.

Finalmente se tiene el CVRF, este pretende dar uniformidad a la forma en la que se avisa cuando se descubren nuevas vulnerabilidades. Cuando se cree que se ha encontrado una vulnerabilidad se le proporciona al fabricante la información precisa, rigurosa y adecuada para que pueda entenderlo y parchearlo de forma eficaz.

Si un atacante encuentra las vulnerabilidades y las explota puede secuestrar el sistema, robar datos o incluso detener el funcionamiento del sistema.

Para minimizar los daños que puedan ocurrir si una vulnerabilidad es explotada por el atacante se pueden realizar copias de seguridad de manera periódica, usar contraseñas seguras, mantener el sistema y los dispositivos actualizados, así como estar al tanto de las nuevas vulnerabilidades que se descubran. Otra buena recomendación es seguir las recomendaciones de las normas que faciliten este tipo de protección, como la norma ISO 27001.

(Ayudaley, 2021; Encyclopedia by Kaspersky, s. f.; Equipo Coremain, 2021; Instituto Nacional de Tecnologías de la Comunicación, s. f.; Ropero, 2015)

3.4.9. Ataques a contraseñas

Una contraseña es una combinación de letras, dígitos y símbolos que se usa para autenticar a un usuario. Los atacantes usan diferentes técnicas y herramientas para atacar las credenciales, y los usuarios siguen muchas malas prácticas que ponen en riesgo su seguridad. Algunas de estas malas prácticas son:

- Utilizar la misma contraseña para diferentes servicios, cuentas o dispositivos.
- Escoger contraseñas débiles o dejar las contraseñas por defecto.
- Usar información personal en la creación de contraseñas, como la fecha de nacimiento, el nombre del usuario, un familiar o mascota.
- Apuntarlas en papel y dejarlo a simple vista.
- Guardar las contraseñas en el navegador.
- Hacer uso de patrones o de secuencias de carácteres.

El objetivo de un atacante siempre será conseguir la información para cometer diferentes delitos, como la obtención de información personal, datos bancarios, suplantación de identidad, entre otros. Los principales ataques a contraseñas son:

- **Ataque de fuerza bruta:** este método consiste en que el atacante intenta acceder a un sistema probando diferentes contraseñas, usando el método de prueba y error. El intruso comienza probando con combinaciones de los datos personales de su víctima si es que tiene información que le sea de utilidad, si esto no funciona, intentan probando diferentes contraseñas hasta que encuentran la contraseña correcta.
- **Ataque de diccionarios:** este método de ataque se aprovecha que las contraseñas suelen ser muy cortas o que usan palabras comunes, para obtenerlas el intruso hace uso de un software que le ayuda a ingresar las contraseñas que hay en un diccionario de manera automática. En este caso un diccionario es un archivo que contiene contraseñas que un usuario podría utilizar, y con el software se va probando de una en una para ver si se encuentra alguna coincidencia.

Protección para evitar ataques a contraseñas.

Para evitar ser víctima de un ataque a contraseña, de deben seguir las siguientes recomendaciones para la creación de contraseñas:

- Usar contraseñas de mínimo ocho caracteres de longitud.
- Usar combinaciones de mayúsculas, minúsculas, números y símbolos.
- No usar palabras sencillas, nombres propios, fechas o lugares.
- No hay que usar secuencias de carácteres (abcd, 12345) o secuencias formadas por los caracteres del teclado (qwerty, asdfgh, zxcvb).

Además del uso de contraseñas robustas, es recomendable usar la autenticación en dos pasos si es que el servicio o aplicación lo permite, ya que esto le dificultaría aún más el acceso al atacante, de igual forma se pueden usar gestores de contraseñas para almacenarlas.

Contraseñas más comunes

De acuerdo con un estudio realizado por la empresa WP Engine, entre las contraseñas más usadas se encuentran:

- 123456
- password
- 12345678
- qwerty
- 123456789
- 12345
- 1234
- 111111
- 1234567
- dragon
- 123123
- baseball
- abc123
- football
- monkey
- letmein
- shadow
- master
- 696969
- michael
- mustang
- 666666
- qwertyuiop
- 123321
- 1234…890
- superman
- 654321
- 1qaz2wsx
- 7777777
- qazwsx
- jordan
- jennifer

También el estudio muestra las secuencias de teclado más utilizadas, entre las cuales están:

- qwerty
- qwertyuiop
- 1qaz2wsx
- qazwsx
- asfgh
- zxcvbnm
- 1234qwer
- q1w2e3r4t5
- qwer1234
- q1w2e3r4
- asdfasdf
- qazwsxedc
- asdfghjkl
- q1w2e3
- 1qazxsw2
- 12QWaszx
- Qweasdzxc
- Mnbvcxz
- a1b2c3d4
- asgjmptw

Hay que tomar en cuenta las medidas de seguridad recomendadas para evitar ser víctimas de un ataque a contraseñas, ya que, si un atacante las obtiene, podría usar la información de la víctima en su beneficio, afectando a la víctima de manera considerable.

(Albors, 2020; Ciberpyme, 2021a; Kelnet Computer, 2021; Ralco Networks, 2020; Valenzuela González, 2022; Vélez Martínez, s. f.; WP Engine, 2024)

3.4.10. Debilidad de los protocolos de red

Un protocolo es un conjunto de reglas que indican como se transmite la información. La ISO es la organización que se encargó de estandarizar la comunicación, para ello creó el modelo OSI, este es un modelo de referencia que indica como se tiene que satisfacer la comunicación de datos para que los fabricantes sean compatibles entre sí. Para que esta comunicación se pueda llevar a cabo, en ambos extremos del canal se debe de tener configurada la misma configuración de protocolos.

El modelo OSI es usado únicamente como modelo de referencia, debido a que el modelo que se usa es el modelo TCP/IP (Transmission Control Protocol/Internet Protocol o Protocolo de Control de Transmisión/Protocolo de internet), el cual se conforma de cuatro capas. La relación entre las capas de ambos modelos se puede observar en la figura 3.15.

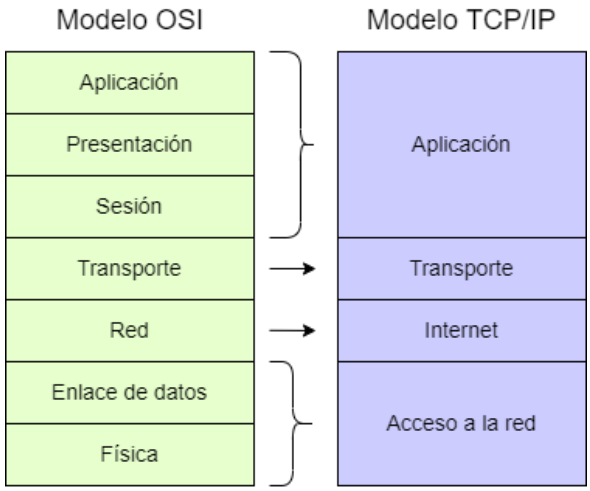


Figura 3.15. Modelo OSI y TCP/IP

Teniendo como referencia lo anterior, todo lo que opera en las capas de acceso a la red, internet y transporte del modelo TCP/IP son considerados protocolos.

Algunos de los protocolos más conocidos por cada capa son:

- Capa de acceso a la red: protocolo ethernet.
- Capa de internet: protocolo IP
- Capa de transporte: protocolos TCP (Transfer Control Protocol o Protocolo de Control de Transmisión) y UDP (User Datagram Protocol o Protocolo de Datagramas de Usuario)

Entre las debilidades de los protocolos mencionados se encuentran:

- **Ethernet:** este es un protocolo de red que controla el método de comunicación entre dispositivos. La IEEE (Institute of Electrical and Electronics Engineers o en español Instituto de Ingenieros Eléctricos y Electrónicos) lo define como el protocolo 802.3. Sobre

este protocolo se construyen las redes de área local o LAN (Local Area Network) y brinda un método de intercambio de datos fiable. Las redes ethernet son ideales para establecer comunicación entre dispositivos cercanos entre sí, esto por las limitaciones de velocidad y la intensidad de la señal, además el tipo de cable influye de manera directa en la velocidad a la que funciona la red, los cables ethernet más comunes son: Cat5, Cat5e, Cat6, Cat6a y Cat7.

Entre las debilidades que puede presentar la capa de acceso a la red se encuentran:

- **Ataques a la tabla MAC:** las tablas MAC (Media Access Control o Control de Acceso a Medios) almacenan la dirección MAC del dispositivo que tienen conectado en una interfaz, esta tabla se almacena en la memoria del switch y son de tamaño fijo. Para realizar un ataque a la tabla MAC, el atacante la llena con direcciones falsas, esto con el propósito de que el switch comience a reenviar todos los paquetes que reciba por todos sus puertos sin tomar como referencia su tabla MAC, de esta manera el atacante puede capturar el tráfico que viaja por la red.
- **Ataques ARP:** el Address Resolution Protocol por sus siglas en inglés ARP o en español, Protocolo de Resolución de Direcciones, vincula una dirección IP con una dirección MAC. En este protocolo no hay forma de que un host pueda validar el origen del paquete que está solicitando su dirección MAC, por lo que esto da lugar a que pueda ocurrir un ataque de ARP Spoofing o ARP poisoning.
- **Ataques de suplantación de direcciones MAC e IP:** la suplantación de dirección IP consiste en que el atacante secuestra una IP válida de un dispositivo de la red objetivo y la comienza a usar como si fuera de él, por lo que puede comunicarse libremente con los dispositivos de la red. En cuando a la suplantación de direcciones MAC, el atacante cambia la dirección MAC de su dispositivo por una MAC que sea de confianza y envía un paquete para que se actualice el puerto al que pertenece la MAC en la tabla de direcciones MAC, por lo que así podrá comenzar a capturar el tráfico que le sea enviado al dispositivo que tiene la dirección MAC que secuestró.

- **Protocolo IP:** el protocolo de internet es considerado la base de internet, proporciona un servicio para la distribución de paquetes de información, su debilidad es que es un protocolo orientado a la no conexión, esto quiere decir que este protocolo no garantiza que el paquete llegue a su destino.

  Otra de las características de este protocolo es que fragmenta los paquetes en caso de ser necesario, ya que el tamaño máximo de un paquete tiene que ser de 65,535 bytes. El protocolo IP proporciona un direccionamiento lógico, es decir, usa las direcciones IP para enviar los paquetes a su destino. La unidad de información de este protocolo es llamada datagrama.

- **TCP – Transfer Control Protocol o Protocolo de Control de Transmisión:** este protocolo es orientado a la conexión, es decir, da garantía de que los paquetes lleguen correctamente a su destino, para esto establece una sesión entre los dispositivos que se quieren comunicar para asegurarse de que el destino está disponible antes de enviar el paquete por completo, además, TCP entrega el paquete en el mismo orden que fue enviado y permite el monitoreo de los datos para impedir que la red se sature.
  Entre las debilidades del protocolo TCP se encuentra que, en las redes inalámbricas, este protocolo no es óptimo, esto porque la comunicación puede alentarse si se producen pérdidas de paquetes durante la transmisión, lo que incrementa el tiempo de carga. Se puede decir que este protocolo es lento, y no tiene un buen rendimiento para transferir de datos en tiempo real.

- **UDP – User Datagram Protocol o Protocolo de Datagramas de Usuario:** este protocolo permite el envío de datagramas sin tener que establecer primero una sesión para saber si el receptor está disponible, es decir, es un protocolo orientado a la no conexión. UDP da soporte a múltiples servicios como DNS (Domain Name Server o Sistema de Nombres de Dominio) y DHCP (Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host). Una debilidad de este protocolo es que no proporciona control de flujo, es decir, si un dispositivo envía la información más rápido que otro es posible que se pierda información, esto va aunado con que UDP no ofrece un control de congestión por lo tanto no tiene la capacidad de reenviar los datagramas que se perdieron en el trayecto, esto lo hace un protocolo no confiable, sin embargo, es más rápido que TCP y es ideal para transmitir datos en tiempo real.

Es importante conocer las debilidades que tiene cada uno de los protocolos, esto con la finalidad de poner en marcha las medidas de seguridad apropiadas en el sistema para que este se encuentre debidamente protegido.

(GeeksforGeeks, 2020; Herramientas WEB, s. f.; KIO One Step Forward, s. f.; Limones, 2021; Riffo Gitiérrez, 2009, p. 14; Weis, 2021)

3.4.11. Ataques a servicios

Un servicio es un medio mediante el cual dos sistemas se comunican, la arquitectura más usada es la cliente – servidor, el cliente envía solicitudes al servidor pidiendo un servicio y el servidor le oferta al cliente el servicio que necesita.

Los servicios se relacionan por medio de una interfaz entre dos capas. Una característica de los servicios que los hace diferentes de los protocolos es que los servicios operan en la capa de aplicación del modelo TCP/IP, además de que usan un puerto.

Algunos de los servicios con sus respectivos ataques son:

3.4.11.1. DNS – Domain Name Server o Sistema de Nombres de Dominio

Este servicio utiliza el puerto 53 TCP y UDP, se encarga de hacer una relación entre las direcciones IP y los nombres de dominio, DNS es útil porque es mucho más fácil recordar el nombre de dominio que su dirección IP.

Los ataques más comunes a DNS son:

- **DNS caché poisoning:** este tipo de ataque consiste en introducir información falsa en un caché DNS para que los usuarios sean redirigidos a sitios web falsos, estos sitios pueden parecer legítimos, por lo que podrían robar información del usuario si éste no se da cuenta que accedió a un sitio falso.
- **Ataque DoS al servidor DNS:** este tipo de ataque es muy común, el atacante satura los servidores DNS y como consecuencia la comunicación con el servidor se complica. Cuando sucede este tipo de ataque y el servidor colapsa, el sitio web al que ofrece servicio queda inactivo.
- **DNS Spoofing:** este ataque consiste en alterar las direcciones IP de los servidores DNS para que la víctima acceda a servidores maliciosos y el atacante pueda obtener la información que necesita.

Para evitar ataques a DNS es recomendable tener instalado software de seguridad, realizar actualizaciones periódicamente en routers y firewalls, además de tener IDS e IPS.

(USS, 2019)

3.4.11.2. DHCP – Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host

Para este servicio, el servidor usa el puerto 67 UDP, y el cliente el puerto 68 UDP. DHCP se encarga de asignar direcciones IP de manera automática a los clientes que lo soliciten. Los clientes le solicitan al servidor una dirección IP, y el servidor guarda en una lista la IP que le asignó al cliente y la dirección MAC del cliente, con esta lista se asegura de que todos los dispositivos tengan direcciones IP diferentes.

Las direcciones que se asignan tienen un determinado tiempo antes de que caduquen, si este tiempo caducó y el cliente necesita seguir usando la dirección IP le tiene que mandar una solicitud al servidor DHCP para extender el tiempo de uso, mientras que, si ya no la necesita, la dirección queda libre para que otro dispositivo pueda usarla.

Los ataques más comunes a DHCP son:

- **Ataque de agotamiento de DHCP:** el atacante satura el servidor DHCP con solicitudes DHCP con el propósito de usar todas las direcciones IP disponibles que tenga el servidor, después de que se agotaron las direcciones, el servidor no podrá asignar direcciones IP a los clientes nuevos, produciendo un ataque DoS, ya que los nuevos clientes no pueden tener acceso a la red.
- **Suplantación de identidad DHCP:** el atacante configura un servidor DHCP falso en la red para proporcionar direcciones IP a los clientes, el propósito de este ataque es obligar a los clientes a usar servidores DNS falsos, para que los clientes usen el dispositivo del atacante como gateway predeterminado.

El ataque de agotamiento de DHCP se suele usar antes del ataque de suplantación de identidad, para facilitar el acceso del servidor falso en la red.

(Institut Sa Palomera, s. f.)

3.4.11.3. Telnet

Telnet proviene del acrónimo Telecomunication Network, ayuda a establecer conexiones remotas con otros dispositivos a través del puerto TCP 23. Surgió en la década de 1960, funciona a través de la terminal y no tiene una aplicación para usarlo en modo gráfico.

Para crear una conexión, se necesita un cliente y un servidor, el cliente será el que envíe la solicitud para iniciar la conexión y el servidor responderá pidiendo las credenciales de acceso del usuario, una vez que el usuario las ingresa correctamente se establece la conexión y ya puede tener acceso remoto al dispositivo solicitado, siempre y cuando el dispositivo destino también tenga activado telnet.

Actualmente se puede decir que Telnet está obsoleto, esto debido a que la información que se transmite entre los dispositivos viaja en texto plano, lo que representa un riesgo de seguridad, y para sustituir a telnet, llegó SSH.

Un atacante puede aprovechar la inseguridad de telnet, por lo que usando herramientas pueden iniciar un ataque de decodificación de contraseñas por fuerza bruta podría obtener las contraseñas vty del switch y acceder remotamente a un dispositivo.

Otro tipo de ataque que puede ocurrir es que el atacante explota un defecto del software del servidor telnet, lo que hace que el servicio no esté disponible, es decir, que ocurra un ataque DoS de telnet, después de que ocurre esto, el administrador no puede acceder remotamente a las funciones de administrador del dispositivo.

(Castillo, 2019)

3.4.12. Denegación de servicios

Un ataque de denegación de servicios tiene como objetivo hacer que un servicio quede indisponible, para lograr esto, el atacante envía muchas solicitudes a un servicio, provocándole sobrecarga, esto se debe a que los servidores tienen un número limitado de usuarios que pueden atender de manera simultánea, por lo que al recibir más solicitudes de las que pueden atender el sistema puede reiniciarse o dejar de responder.

Hay dos tipos de ataque de denegación de servicios:

- **DoS – Denial of Service o Denegación de Servicio:** Este tipo de ataque se lleva a cabo desde un único origen, por lo que detener este ataque resulta sencillo, ya que hay que identificar cual es la dirección IP que está haciendo las peticiones masivas al servidor, y una vez identificada hay que bloquear esa IP para que ya no tenga acceso, desapareciendo así la sobrecarga
- **DDoS – Distributed Denial of Service o Denegación de Servicios Distribuido:** a diferencia de DoS, este ataque es realizado desde diferentes orígenes, por lo que resulta más difícil detenerlo. Para realizar este ataque, el intruso envía un virus a diferentes computadoras, con este virus el atacante puede hacer uso de los recursos de hardware de las víctimas infectadas para enviar múltiples solicitudes al servidor objetivo, estas computadoras infectadas reciben el nombre de botnet.

Hay tres modos de ataque de denegación de servicios:

- **Consumo de recursos:** Para que los dispositivos de la red funcionen adecuadamente necesitan tener ciertas características, como ancho de banda, tiempo de procesamiento, espacio de disco, entre otros, por lo que si a algún dispositivo de red se le agotan los recursos no va a funcionar adecuadamente o puede dejar de funcionar. Hay dos métodos por los que se puede realizar un ataque de denegación de servicios por consumo de recursos:
    - **Por explotación de vulnerabilidades:** se aprovechan de las vulnerabilidades del sistema para volverlo inestable, por lo que se envían paquetes mal intencionados puede ocurrir un escenario que no se tenía previsto, el cual puede provocar que se ralentice la velocidad de ejecución del servicio, se reinicie o comience a consumir grandes cantidades de memoria, para finalizar en una denegación de servicio.
    - **Por saturación o inundación:** estos envían una gran cantidad de solicitudes falsas al sistema con la finalidad de saturarlo y que no pueda responder a las solicitudes reales. La fortaleza de estos ataques está en el envío de grandes cantidades de tráfico en su contenido.
- **Destrucción o alteración de la información de configuración:** Si los dispositivos no están bien configurados pueden dejar de funcionar de manera adecuada o dejar de

funcionar por completo, por lo que si el atacante consigue destruir o modificar la información de configuración de los dispositivos puede provocar una denegación de servicios.

- **Destrucción física o alteración de componentes de red:** Si el intruso consigue acceder físicamente a las instalaciones o equipos de red puede realizar un gran número de ataques que provoquen una denegación de servicios, como la interrupción del suministro eléctrico, desconexión o apagado de equipos, vandalismo, robo o alteración de los componentes.

Ejemplos de ataques de denegación de servicios

- **ICMP Flood:** también conocido como ataque de inundación de ping. En este tipo de ataque, el intruso intenta saturar un dispositivo con solicitudes ICMP. Los mensajes ICMP se usan para hacer ping a un dispositivo de red con el fin de diagnosticar el estado de la conexión entre el remitente y el emisor, por lo que cuando el atacante satura el objetivo con mensajes ICMP la red se ve obligada a responder cada uno de los mensajes recibidos, por lo que la red se vuelve inaccesible para el tráfico normal.
- **HTTP Flood:** en este tipo de ataque, el intruso explota solicitudes HTTP GET o POST para atacar un servidor web o una aplicación. Este tipo de ataque usa menos ancho de banda para inhabilitar a la víctima o tomar el control. El uso más habitual de este ataque es usar el dispositivo víctima para atacar otros dispositivos de la red o para ampliar la red de botnets del atacante.
- **Slowloris:** este es un ataque de capa de aplicación que realiza solicitudes HTTP parciales para abrir conexiones entre una computadora y el servidor web objetivo. Este ataque mantiene abiertas las conexiones el mayor tiempo posible, con la finalidad de ralentizar el equipo víctima. Slowloris requiere un ancho de banda mínimo para iniciarse y solo afectar al servidor web objetivo sin afectar otros servicios o puertos.
- **Smurf:** en este tipo de ataque, el intruso satura el dispositivo objetivo con paquetes ICMP. Para hacerlo, el atacante falsifica la IP del objetivo y envía mensajes ICMP que tengan como IP fuente la IP falsificada, así al enviar los paquetes ICMP los dispositivos que respondan enviarán la respuesta al dispositivo víctima por lo que el dispositivo víctima se sobrecargará de solicitudes, lo que hará que quede inaccesible. Cabe mencionar que este tipo de ataque ya no es muy frecuente, debido a que puede considerarse como una vulnerabilidad resuelta.

Medidas de protección frente a los ataques de denegación de servicios

Implementar medidas de seguridad para prevenir los ataques de denegación de servicios son muy importantes, por lo que se aconseja el uso de las siguientes medidas de protección:

- Es recomendable ubicar el servidor en la DMZ (Demilitarized Zone o Zona Desmilitarizada), para evitar que el atacante pueda acceder a la red interna si vulnera el servidor.

- Se tienen que implementar IDS e IPS, para monitorizar las conexiones y alertar de intentos no autorizados o un mal uso de protocolos.
- Se recomienda tener el mayor ancho de banda posible, esto para que el sistema pueda gestionar los picos de tráfico causados por la denegación de servicios.
- Es importante contar en la red con redundancia y balance de carga.
- Los dispositivos deben estar actualizados y contar con antivirus.
- Hay que dimensionar adecuadamente la forma de los sistemas, para evitar ataques de denegación de servicios de manera accidental por parte de los usuarios.

(Imperva, s. f.; NETSCOUT, s. f.-a; UNAM, s. f.-b; Verdejo Álvarez, s. f.)

3.4.13. Ataques a redes inalámbricas

Las redes inalámbricas son muy usadas en la actualidad debido a la flexibilidad que proporcionan, ya que eliminan la necesidad de conectarse a la red por medio de cables, sin embargo, también se debe estar consciente de que hay muchos riesgos que se pueden correr al navegar haciendo uso de una red inalámbrica.

Debido a que la comunicación inalámbrica usa el aire como medio de transmisión, hace posible que cualquier persona conectada a la red pueda ver el tráfico que viaja por la misma, siendo esta una desventaja en comparación de las redes que usan cables como medio de transmisión.

También hay que tener en cuenta que la conexión a la red inalámbrica solo se da en el área de cobertura de la red, y entre más distancia haya entre el emisor y el receptor la velocidad de transmisión disminuirá, asimismo, los elementos intermedios como paredes, campos magnéticos o electrónicos pueden interferir con la calidad de la transmisión, también puede verse afectada la calidad de transmisión si hay un número elevado de usuarios conectados.

Ventajas y desventajas de las redes inalámbricas

Las ventajas que tienen las redes inalámbricas sobre las redes cableadas son:

- **Movilidad:** los dispositivos van a poder conectarse a la red sin necesidad de usar un cable solo si están dentro del área de cobertura.
- **Desplazamiento:** los usuarios con dispositivos conectados a una red inalámbrica pueden moverse libremente por su área de cobertura sin perder la conectividad.
- **Flexibilidad:** permite colocar los dispositivos en diferentes lugares sin hacer alguna configuración adicional, esto muestra una clara ventaja sobre las redes cableadas, ya que los costos se elevan si se quiere extender la red. Asimismo, se elimina la necesidad de poner cables provisionales en el piso, con los cuales alguna persona podría accidentarse o el cable podría ser dañado accidentalmente por algún usuario.

- **Reducción de costos:** es más costoso diseñar una red cableada que una red inalámbrica, además de costos, se reduce el tiempo de instalación de la red.
- **Escalabilidad:** es muy fácil conectar nuevos dispositivos a la red, a diferencia de las redes cableadas, que se tendría que instalar un nuevo cable si no se tiene uno listo para usarse.

Las desventajas de las redes inalámbricas son:

- **Menor ancho de banda:** entre más dispositivos conectados haya, disminuirá el ancho de banda para cada uno de ellos.
- **Mayor inversión inicial:** el costo de los dispositivos inalámbricos es más costoso que los dispositivos de las redes cableadas.
- **Seguridad:** el aire al ser el medio de transmisión de este tipo de redes se tiene como desventaja que si un atacante se conecta a la red inalámbrica podrá ver el tráfico que circula por ella.
- **Interferencia:** las redes inalámbricas funcionan en una banda de frecuencia de 2.4 GHz, la cual no requiere de una licencia administrativa para usarse, por lo que muchos dispositivos dentro del mercado como teléfonos inalámbricos y microondas usan esta misma banda de frecuencias, por ende, entre más interferencia se produzca por otros dispositivos, el rendimiento de la red disminuirá.

Vulnerabilidades de las redes inalámbricas

Los ataques a este tipo de redes son muy comunes, los atacantes hacen uso de diferentes softwares y herramientas que le proporcionan al intruso métodos para evitar las medidas de seguridad implementadas. De manera general, los ataques a redes inalámbricas se basan en interponerse en la comunicación del emisor y el receptor, para monitorizar y robar datos.

Algunos de los ataques a las redes inalámbricas son:

- **Redes trampa:** este tipo de ataque consiste en crear una red inalámbrica similar a la original, estas redes se crean usando software y hardware. Este tipo de redes suelen colocarse en lugares con una gran afluencia de usuarios, de tal forma que la red pueda pasar desapercibida y engañe al mayor número de usuarios posible. El objetivo de este tipo de redes es robar información personal de los usuarios conectados, además de esto, el atacante puede tomar el control sobre la navegación, por lo que puede hacer que la víctima acceda a páginas fraudulentas para posteriormente infectar el dispositivo con malware.
- **Envenenamiento de Cookies:** una cookie es un dato específico de un sitio web y de una sesión del usuario que incluye información de interés o de identidad de los usuarios y éstas se almacenen en su navegador. Los servidores pueden usar las cookies para llevar un seguimiento de las tendencias de uso.

Los atacantes pueden interceptar las cookies antes de que vuelvan al servidor para extraer la información o modificarla, asimismo, se pueden crear cookies falsas desde cero, esto para suplantar la identidad de un usuario o burlar la seguridad de un servidor.

- **Ataques Man – In – The – Middle:** este tipo de ataque está fuertemente asociado a conexiones inalámbricas inseguras. En este tipo de ataque hay un intermediario que se encuentra entre el emisor y el receptor, de esta forma puede interceptar los datos que viajan entre los dispositivos y la red.
- **Robo de datos:** en las redes inalámbricas públicas, muchas veces se pide información para poder acceder a ellas, por ejemplo, correo electrónico o número de teléfono. Cuando el usuario proporciona su información el atacante puede interceptarla para después usarla con diferentes motivos, como suplantación de identidad o realizar un ataque de phishing personalizado.

Proteger las redes inalámbricas

La protección de estas redes también es importante, por lo que se sugieren las siguientes medidas de protección para navegar de forma segura:

- **Cambiar los valores predeterminados de inicio de sesión:** algunos de los fabricantes en sus dispositivos incluyen contraseñas de administrador y nombres de red predeterminados, otros lo escriben directamente en la carcasa del dispositivo, esto facilitaría a un atacante el acceso a la red, por lo que es importante que cuando la red sea configurada por primera vez se cambie el nombre de red y se cree una contraseña que cumpla con los parámetros de seguridad establecidos.
- **Activar el firewall:** el firewall del router regula el paso de tráfico en la red, previniendo que tráfico no deseado ingrese a la red. Una medida de protección es habilitar el modo sigiloso para bloquear el tráfico ICMP, también conocido como ping, de esta forma ya no se podrá acceder a los datos privados de la red o escanearla para detectar sus vulnerabilidades.
- **Actualizar frecuentemente el firmware:** hay que mantener actualizado el firmware, para que se tengan las actualizaciones de seguridad proporcionadas por el fabricante, las cuales ayudarán a mantener la red más segura.
- **Actualizar software:** mantener actualizado el software de los dispositivos es otra medida para reducir la obtención de información por parte de los atacantes.

La información es lo más valioso tanto de las organizaciones como de los usuarios, por lo que es importante protegerla para evitar que los atacantes obtengan información que puede perjudicar enormemente a las víctimas.

(Ciberpyme, 2021b; F5, Inc., s. f.; J. Jiménez, 2021a; Tecnocosas, 2018; Teoyotl Calderón, 2013)

3.5. Mantener acceso a sistemas comprometidos

3.5.1. Puertas traseras

Una puerta trasera, o backdoor es un malware que explota una vulnerabilidad para proporcionar a los atacantes acceso remoto al dispositivo infectado, y una vez dentro pueden realizar todo tipo de actividades en dicho dispositivo.

Los backdoors son invisibles para el usuario, cuando el sistema inicia se ejecutan silenciosamente, además, para que no sea detectado fácilmente hace uso de un programa blinder.

De manera general se tienen dos tipos de puertas traseras:

- **Las que intentan instalarse de manera externa en el sistema:** estas pueden ser creadas por los atacantes para instalarlas en el sistema de su interés, con el propósito de acceder a la información almacenada e incluso afectar el rendimiento de los dispositivos.
- **Las que están presentes en el software y/o programas legítimos:** existe la posibilidad de que los backdoors estén previamente instalados en el sistema o aplicaciones, esto porque el desarrollador pudo haber olvidado quitarlas o bloquearlas, aunque también existe la posibilidad de que las haya dejado a propósito, si este es el caso, pueden ser usadas con fines benéficos como la realización de mantenimiento o solucionar problemas remotamente. Una puerta trasera de este tipo no debería representar un problema de seguridad si proporciona acceso únicamente a usuarios de confianza.

Las puertas traseras también se pueden clasificar de la siguiente forma:

- **Basadas en software:** como su nombre lo indica, éstas se ejecutan exclusivamente en el software, por lo que es más fácil que sean detectadas por el software antivirus, o como ya se mencionó anteriormente, pueden haberse instalado para realizar actividades de manera remota, sin que esto represente un riesgo.
- **Basadas en hardware: estas se aprovechan de una pieza de hardware:** este tipo de puertas traseras se aprovechan de los componentes de hardware, se inserta un código malicioso en algún componente de hardware mediante el cual los atacantes podrían acceder a los sistemas protegidos. Se considera que las puertas traseras basadas en hardware son mucho más peligrosas que las que están basadas en software, ya que al estar en piezas de hardware alteradas los antivirus no son capaces de detectarlas, además de que para este tipo de backdoors los archivos que se encuentran cifrados o las contraseñas no son un problema.

Detectar un backdoor es complicado, ya que puede ser confundido con un virus, sin embargo, debe ponerse atención a ciertas señales que indiquen que algo pasa en el dispositivo. Algunas de estas señales son:

- El rendimiento del dispositivo ha disminuido.
- La velocidad de navegación en internet es más lenta de lo normal.
- Continuamente aparecen ventanas emergentes que piden actualizar información o ingresar nombres de usuarios y contraseñas.

Para protegerse de un backdoor es necesario el uso de un antivirus que proporcione protección en tiempo real, además es necesario mantenerlo actualizado para poder detectar correctamente nuevas amenazas, también es necesario tener instalada la última versión del sistema operativo.

Adicionalmente hay que usar el sentido común al navegar por internet, esto para evitar descargar archivos maliciosos de fuentes desconocidas o acceder a páginas poco confiables, además hay que asegurarse de la autenticidad de los correos electrónicos que se reciben y descargar archivos únicamente de sitios oficiales.

(Albors, 2015; Grupo Atico34, 2020b)

3.5.2. Caballos de troya

Un caballo de troya o troyano es un software malicioso que aparenta ser un programa legítimo, por lo que los usuarios creen que dicho software es seguro e inofensivo, sin embargo, al momento de ejecutarse le permite al atacante acceder remotamente al equipo infectado. Su nombre proviene del caballo de madera que se usaba para engañar a los defensores de troya para introducir soldados a escondidas en la ciudad.

Un troyano se hace pasar por un archivo legítimo, por lo que es fácil engañar a las víctimas para que hagan clic en el e instalen el software, al hacer esto, el troyano comienza a funcionar, por lo que instala malware en el dispositivo, para espiar o causar peores daños a la víctima.

Algunos de los tipos de troyanos más comunes son:

- **Troyanos de puerta trasera:** pueden crear backdoors en el dispositivo de la víctima, lo que permite que el atacante pueda instalar más malware, espiar a la víctima o conectar su dispositivo a la red de bots del atacante.
- **Troyanos de descarga:** tienen como objetivo descargar más software malicioso en el equipo infectado.
- **Troyanos exploit:** usan exploits para aprovechar vulnerabilidades de software o hardware para infectar el dispositivo víctima.

- **Troyano infostealer:** tiene como objetivo robar datos personales y enviarlos al atacante, quien puede usarlos para hacer algún fraude o robar la identidad de la víctima.
- **Troyano de ataque DDoS:** ejecuta ataques DDoS, para que la red se sature y deje de funcionar, además agregan el dispositivo atacado a su red de bots.

Para reconocer si se tiene instalado un troyano en el dispositivo se tiene que poner atención a las siguientes señales:

- **El dispositivo se vuelve lento:** esto porque los troyanos instalan otro malware, lo que puede causar que el dispositivo consuma muchos recursos.
- **Bloqueo del sistema:** los troyanos pueden saturar el dispositivo, provocando que este se bloquee o falle de diversas maneras, como, por ejemplo, la pantalla azul de Windows puede deberse a problemas con drivers, antivirus e incluso a problemas con el hardware, la presencia de troyanos puede hacer que el sistema operativo colapse, por lo que el dispositivo puede verse obligado a apagarse o reiniciarse de forma inesperada, y la pantalla azul aparece como una medida de seguridad para evitar que por dicho fallo se dañen otras partes del sistema.
- **Instalación de aplicaciones desconocidas:** hay que poner atención a las aplicaciones, ya que como se mencionó, los troyanos descargan otro malware.
- **Redireccionamiento en internet:** algunos troyanos pueden cambiar la configuración DNS para redirigir a la víctima a sitios maliciosos para recopilar más información o instalar más malware.

Para protegerse de los troyanos se tiene que hacer uso de un software antivirus, con el cual se pueden analizar los archivos antes de descárgalos, también hay que evitar abrir archivos adjuntos o abrir enlaces recibidos, el correo electrónico es el método de distribución más común de este tipo de malware. Otra recomendación es mantener actualizado el software y el sistema, para contar con los parches de seguridad proporcionados por el proveedor.

Muchas veces troyanos y backdoors son confundidos y se cree que son lo mismo, sin embargo, no es así, la diferencia está en que los troyanos tienen funcionalidades de backdoor, por lo que pueden introducirse en el dispositivo víctima y actuar sin levantar sospechas, mientras que los backdoors no siempre provienen de fuentes externas, muchos de ellos están incorporados nativamente en el sistema o aplicaciones de la víctima.

(Eset, s. f.; F-Secure, s. f.; Muñoz, 2017; Norton, 2018b)

3.5.3. Rootkits

Un rootkit es un software malicioso que permite el acceso no autorizado a un dispositivo, estos son difíciles de detectar y pueden ocultar su presencia. La mayoría de los rootkits afectan el

software y el sistema operativo, aunque hay algunos que también pueden infectar el hardware y el firmware.

Este malware es usado por los atacantes para acceder remotamente a un dispositivo, con el fin de manipularlo o robar datos, además tienen como propósito conseguir acceso privilegiado a nivel del administrador del sistema, por lo que puede realizar las mismas modificaciones que el administrador.

Un rootkit puede realizar lo siguiente:

- Oculta otros tipos de malware, lo que a su vez dificulta su eliminación.
- Proporciona acceso remoto al mismo tiempo que evita ser detectado.
- Puede manipular o desactivar programas de seguridad, es decir, puede apagar por completo los programas de seguridad de un equipo.
- Pueden crear un backdoor permanente, lo que le permite acceso al atacante cada que lo requiera.

Generalmente los rootkits se clasifican en seis categorías:

1. **Rootkits de modo de usuario:** infectan la cuenta del administrador del sistema operativo, por lo que obtienen los privilegios de máximo nivel y pueden cambiar los protocolos de seguridad del dispositivo. Estos afectan solamente el software del dispositivo, por lo que son los más fáciles de detectar y de eliminar.
2. **Rootkits de modo kernel:** estos residen en el mismo nivel que el sistema operativo. Cuando se instala un rootkit de este tipo todo está contaminado, por lo que realizar un análisis antirootkit es inútil, ya que no sería detectado. Si un atacante logra instalar un rootkit de este tipo, además de tener acceso a los archivos del dispositivo puede cambiar el funcionamiento del sistema operativo. Cabe mencionar que este tipo de rootkit es difícil de crear, ya que si está mal creado puede causar bloqueos en el sistema y problemas de funcionamiento que revelen que hay un rootkit instalado.
3. **Rootkits híbridos:** estos tienen algunos componentes a nivel de usuario y otros a nivel de kernel.
4. **Rootkits de firmware:** estos tienen la capacidad de esconderse en el firmware cuando el equipo se apaga, por lo que al encenderse son capaces de reinstalarse y regresar a trabajar. Los rootkits de firmware son capades de infectar el disco duro o la BIOS del sistema.
5. **Bootkits:** son una variante de los Rootkits de modo kernel que infectan la MBR (Master Boot Record o Registro de Arranque Maestro) del dispositivo. Estos han quedado obsoletos, ya que Windows 8 y Windows 10 tienen la función de arranque seguro, sin embargo, dispositivos con Windows 7 siguen estando en riesgo.
6. **Rootkits virtuales:** se cargan en el sistema operativo original y después ponen el sistema operativo en una máquina virtual, estos son difíciles de detectar porque se ejecutan de manera independiente del sistema operativo del equipo.

Un rootkit necesita ayuda para instalarse, por lo que los atacantes los empaquetan con dos programas asociados: el dropper y el loader.

- **Dropper:** es la primera fase del proceso de instalación, este es el que importa el rootkit al dispositivo víctima y activa al loader.
- **Loader:** se encarga de instalar el rootkit en el sistema destino, cuando lo hace por lo regular provoca un desbordamiento de búfer.

Hay algunas señales que pueden alertar al usuario de que se ha instalado un rootkit en un dispositivo:

- El dispositivo se comporta de manera extraña.
- Hay cambios no autorizados en la configuración del dispositivo, por ejemplo, hora y fechas incorrectas.
- La conexión a internet falla más de lo habitual.
- La memoria RAM tiene un rendimiento más bajo.
- Frecuentemente aparece la pantalla azul.

Para evitar que se instale un rootkit hay que tomar medidas de seguridad similares a las mencionadas anteriormente, entre las que se incluyen: revisar que los archivos que se descargan provengan de una fuente confiable, también se deben de tener instaladas las actualizaciones de seguridad del sistema operativo y mantener actualizadas las aplicaciones que se usan.

(Burdova, 2021; Moes, 2023; Rivero, 2009)

3.5.4. Cryptojacking

Las criptomonedas, criptodivisas o criptoactivos son monedas digitales o virtuales, que mediante el uso de métodos criptográficos verifican las transacciones para hacerlas más seguras. A diferencia del dinero tradicional, las criptomonedas usan un sistema descentralizado, es decir, no están controladas por alguna institución y para realizar transacciones no se requiere de intermediarios y para el control de las transacciones se usa una base de datos descentralizada o blockchain.

Entre las criptomonedas más conocidas se encuentran:

- **Bitcoin:** fue la primera criptomoneda, desarrollada en 2009 por Satoshi Nakamoto, éste es un seudónimo para una persona o un grupo de personas, ya que actualmente sigue sin saberse el origen preciso del bitcoin. Actualmente es la criptomoneda más conocida y comercializada.

- **Ethereum:** también conocida como Ether o ETH, fue desarrollada en 2015, por la plataforma de blockchain Ethereum. Junto con el bitcoin es de las criptomonedas más conocidas

La adquisición de criptomonedas puede hacerse mediante intercambios, también pueden comprarse usando dinero convencional en páginas especializadas, sin embargo, existe un proceso mediante el cual también se pueden adquirir criptomonedas, el cual es llamado minería o mining. El minado de criptomonedas requiere de una gran capacidad de cómputo, ya que se usan muchos recursos informáticos para resolver problemas matemáticos complicados, los cuales generan criptomonedas.

Quienes usan criptomonedas suelen hacerlo por los diferentes beneficios que ofrecen, entre ellos: evitar los cargos adicionales que cobran los bancos por realizar algunos tipos de transacciones, también podrían ser usadas porque ofrecen anonimato e incluso hay quienes prefieren adquirirlas para conservarlas, esperando que su valor aumente.

El minado de criptomonedas al requerir una gran cantidad de recursos computacionales representa un gasto, no solo de hardware, sino también de energía y a raíz de esto es como surge el cryptojacking. Éste es un delito informático mediante el cual un atacante también denominado cryptojacker genera criptomonedas utilizando silenciosamente los recursos computacionales de sus víctimas, al hacer esto los cryptojackers reducen los costos y obtienen criptomonedas para su beneficio.

Los cryptojackers para ingresar al dispositivo víctima pueden hacerlo de las siguientes maneras:

- Mediante un correo electrónico envían un enlace malicioso a la víctima, quien sin saber que el enlace es malicioso hace clic en él, en cuanto esto sucede, el código malicioso que contiene se carga en el dispositivo, para posteriormente comenzar con el minado de criptomonedas de manera silenciosa.
- Otra forma de infectar un dispositivo es inyectando código malicioso JavaScript en un anuncio o sitio web, dicho código se ejecuta inmediatamente después de que la víctima carga el sitio en su navegador.

Después de que el atacante logró ingresar al dispositivo de la víctima, instala un software de cryptojacking el cual se ejecuta en segundo plano, y con los recursos del dispositivo en cuestión comienza a generar criptomonedas y roba las que encuentre almacenadas. Algunos de los softwares de cryptojacking podrían comportarse como gusanos, por lo que una vez dentro de la red o sistema intentaran infectar a otros dispositivos.

Las víctimas del cryptojacking pueden notar problemas en el rendimiento de sus dispositivos, como reducción en la velocidad de los procesos o sobrecalentamiento de las baterías de los dispositivos y al estar usando una mayor capacidad de cómputo, los costos por consumo de electricidad también aumentan.

Hay algunas formas con las cuales se puede prevenir ser víctima de criptojacking, entre las cuales se encuentran:

- Actualizar el sistema operativo de los dispositivos, así como instalar los parches de seguridad.
- Evitar descargar software de sitios no seguros.
- Evitar el uso de redes wifi públicas.
- Instalar un antivirus confiable y mantenerlo actualizado.

(Interpol, s. f.; Kaspersky, 2023a; Malwarebytes, s. f.; Proofpoint, 2022; Ribas, 2022)

3.6. Eliminación de evidencias

3.6.1. Eliminación de evidencias

Una evidencia es un elemento que no ha pasado por un proceso de identificación y análisis, por lo que es diferente de una prueba, ya que para que una evidencia se convierta en prueba tiene que pasar por dicho proceso de identificación y análisis. En informática, una evidencia puede ser: una memoria USB, un DVD, entre otros elementos.

No todas las evidencias logran convertirse en pruebas, los peritos informáticos son los que se encargan de realizar el análisis de las evidencias, para esto hacen uso de herramientas forenses. Cabe mencionar, que una evidencia puede poner al descubierto la identidad de un atacante después de ser analizada, de aquí surge la importancia de su eliminación.

Cuando un atacante pretende eliminar o destruir una evidencia lo hace con el propósito de imposibilitar su recuperación para evitar dejar un rastro que ponga al descubierto su identidad, la eliminación de evidencias puede llevarse a cabo de las siguientes maneras:

- **Desmagnetización:** este método puede aplicarse para destruir datos almacenados en los dispositivos magnéticos, como discos duros, disquetes o cintas magnéticas. La desmagnetización consiste en exponer los soportes de almacenamiento a campos magnéticos potentes de acuerdo con su tamaño y forma ya que cada tipo de dispositivo necesitará una potencia magnética específica para asegurar la polarización de las partículas y así eliminar por completo la información.
- **Destrucción a nivel físico:** el propósito de este tipo de destrucción es dejar inutilizable un dispositivo y así evitar que se recupere información que revele la identidad del atacante. Para destruir físicamente un dispositivo se pueden realizar diferentes técnicas, como la desintegración, pulverización o incineración. Si este proceso se lleva a cabo correctamente la posibilidad de recuperar la información se vuelve prácticamente imposible.
- **Sobre escritura:** este método consiste en escribir información sobre los datos que están almacenados en un dispositivo, para asegurar la total destrucción de los datos debe de sobre escribirse en toda la superficie de almacenamiento. La sobre escritura modifica los valores almacenados, por lo que este método no puede realizarse en dispositivos que están dañados o en aquellos que son regrabables.

Las evidencias son elementos sensibles, por lo que, si una persona inexperta trata con ellas, puede dañarlas irreversiblemente, esto ocasionaría que el proceso de eliminación y análisis no se pueda llevar a cabo o se lleve a cabo incorrectamente, y como consecuencia, la evidencia no se podría convertir en prueba.

(Vásquez, 2016)

3.6.2. Ocultar información

La información es el activo más valioso, no solo de una organización, sino de cualquier persona en general, por lo que es muy importante mantenerla segura, si la información está en riesgo, se pueden tener graves consecuencias, las cuales pueden afectar enormemente a las víctimas.

El propósito de ocultar información es hacerla lo menos visible y accesible posible, para lograr esto se puede hacer uso de diferentes técnicas, como el covert channel, la criptografía y también la esteganografía.

- **Covert channel:** es una forma de comunicación mediante un sistema que no fue diseñado para procesos de comunicación, su objetivo es proteger la privacidad o aumentar la seguridad de la comunicación, sin embargo, esto también es una desventaja, ya que al proporcionar un canal de comunicación sigiloso se puede establecer una conexión que esté prohibida por las políticas de seguridad, esta característica también puede ser aprovechada por un atacante para extraer información de sus víctimas.
  La creación de un covert channel implica programación ingeniosa y acceso al sistema de archivos, y para detectar uno se tiene que hacer un análisis del rendimiento del sistema, esto porque los covert channel pueden degradar el rendimiento del sistema, pero con el avance de la tecnología esta degradación es insignificante si se compara con todos los datos que procesa el sistema, por lo que detectarlo se vuelve complicado.
  Una forma en la que una organización puede protegerse de un covert channel es hacer un análisis de los recursos que se están usando en el sistema para así monitorear su rendimiento para que en caso de detectar un comportamiento inesperado se encuentre una solución rápida o se sepa de donde viene dicho comportamiento.

- **Criptografía:** el término criptografía proviene del griego *kryptos* cuyo significado es ocultar y *grafos* que significa escribir, por lo que criptografía significa *escritura oculta.*
  La criptografía se basa en técnicas matemáticas que se usan para cifrar y descifrar información. El término cifrar se usa para ocultar la información, mientras que descifrar se refiere proceso que se sigue para volver a hacer legible la información para el receptor.
  Los tipos de criptografía son:
  - **Criptografía de clave secreta o criptografía simétrica:** se usa una sola clave, con la cual se cifran y se descifran los datos, esto significa que el emisor y el receptor conocen dicha clave. La seguridad de este tipo de criptografía radica en que la clave debe mantenerse en secreto.
  - **Criptografía de clave pública o criptografía asimétrica:** el emisor y el receptor tienen dos claves, una privada y una pública, con las cuales se puede establecer un canal de comunicación seguro. Para usar este tipo de criptografía ambas partes de la comunicación deben de compartir sus claves públicas, ya que estas claves son las que se usarán para cifrar la información que intercambiarán,

mientras que para descifrar la información, deberán hacerlo usando su clave privada, en otras palabras, si el usuario A quiere comunicarse con el usuario B, el usuario B debe compartir con A su clave pública, así A podrá cifrar la información con la clave pública de B y B podrá descifrarla usando su clave privada.

La criptografía es un método muy usado para proteger la información, para que solo el destinatario pueda descifrarla para obtener el mensaje original que le fue enviado.

- **Esteganografía:** es un método que se usa para ocultar información en un objeto portador. A diferencia de la criptografía que busca hacer que la información sea ilegible, la esteganografía busca ocultar la información en otro objeto, el cual lleva por nombre contenedor.

  En la antigüedad, la esteganografía fue usada para ocultar información en el contenedor usando diferentes técnicas y herramientas, las cuales se describen un poco más a detalle en el siguiente tema.

(Agencia SINC, 2017; Álef, 2017; Cilli, 2017; Grupo Atico34, 2020a; Marín, 2019; Medina Velandia, 2017; Velasco Bautista et al., 2007)

3.6.3. Esteganografía

La palabra *esteganografía* proviene de las palabras *steganos* que significa *oculto* o *cubierto* y *graphia* que significa *escritura,* por lo que esteganografía se define como el arte o la ciencia de comunicar información de manera oculta, esta usa un conjunto de técnicas para ocultar información en un contenedor, que puede ser un archivo, una imagen, algún programa ejecutable, entre otros, así, el mensaje puede ser enviado de manera segura y solo puede ser recuperado por el usuario a quien va dirigido el mensaje ya que dicho usuario sabe qué algoritmo usar para extraer la información.

Los componentes de la comunicación usando esteganografía son:

- **Contenedor:** es el objeto que se utiliza para cubrir el mensaje, como una imagen, un texto, un audio o vídeo, de manera general, este contenedor no levanta ninguna sospecha.
- **Mensaje:** es el mensaje que se quiere enviar.
- **Esteganograma:** es el contenedor que lleva el mensaje oculto que se va a transmitir.
- **Clave esteganográfica:** es el algoritmo o método de extracción que usa el receptor para recuperar el mensaje oculto.

El proceso que se sigue para ocultar un mensaje usando esteganografía puede observarse en la figura 3.16:

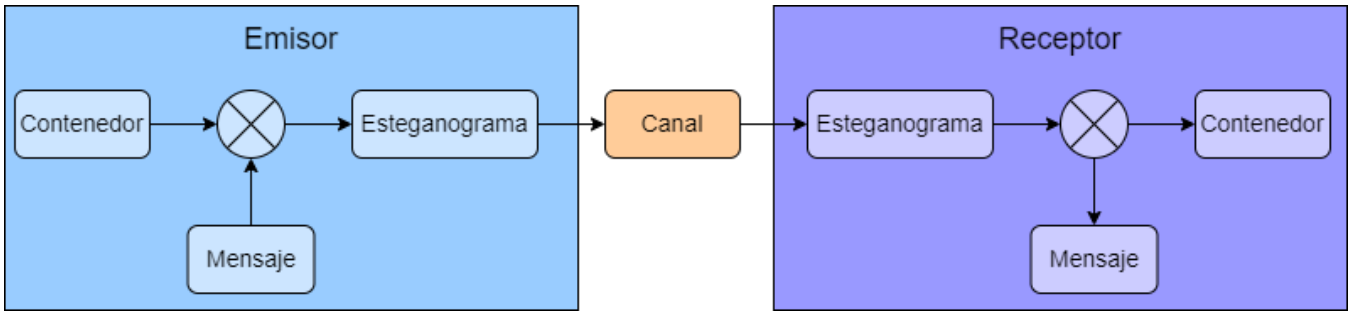


Figura 3.16. Proceso esteganográfico

(Velasco Bautista et al., 2007)

El contenedor y el mensaje mediante alguna técnica se unirán formando el esteganograma, el cual viajará mediante un canal, dicho canal puede ser seguro o inseguro, después de que el esteganograma llega al receptor, se tiene que hacer el proceso inverso para que el receptor obtenga el mensaje oculto que le fue enviado.

Esteganografía clásica y esteganografía moderna

En la esteganografía clásica se usan técnicas manuales, sin fuentes tecnológicas, mientras que en la esteganografía moderna se usan canales digitales, como imágenes, audios, videos, entre otros.

El término esteganografía fue usado por Johannes Trithemius en su libro publicado en el año 1500, donde codificó varios mensajes que fueron descubiertos hasta el año 1996, sin embargo, alrededor del año 430 a.C, Herodoto de Halicarnaso en su libro “Las historias” reflejó el uso de la esteganografía, y en el año de 1641, John Wilkins publicó su libro *Mercury,* donde mostraba como dos músicos se podían comunicar tocando sus instrumentos musicales.

Otro momento donde la esteganografía se usó con éxito fue durante la Primera Guerra Mundial, una de las técnicas de amplia difusión fue la tinta invisible, mientras que la técnica más usada durante la Segunda Guerra Mundial fue la de los micropuntos, en esta técnica se reducían fotos hasta que fueran del tamaño de un punto de 1mm de diámetro, estos micropuntos eran cortados con una aguja o punzón y se pegaban en un texto, ésta fue una técnica bastante buena y fue descubierta hasta el año 1941.

Otra técnica de esteganografía clásica fue la de la rejilla de cardano, en donde se usaba una rejilla de tal manera que al ponerse sobre un texto los agujeros resaltaban ciertas palabras, las cuales formaban el mensaje oculto.

La esteganografía moderna surgió en el año de 1985, Barrie Morgan y Mike Barney, ingenieros de Datotek propusieron una forma segura de enviar información mediante canales restrictivos de comunicación.

Un ejemplo de esteganografía moderna fue el que usaron los terroristas Al-Qaeda en 2011 en Berlín, donde se les decomisó una tarjeta de memoria que contenía una carpeta protegida con una contraseña, cuando la policía logró descifrar la contraseña encontró un video, y fue bastante extraño que la tarjeta de memoria tuviera contraseña para ocultar un video, por lo que siguieron investigando, hasta que consiguieron extraer del video 141 archivos de texto donde venía información relevante de Al-Qaeda y sus planes futuros.

En la esteganografía moderna hay diferentes métodos para ocultar información en distintos archivos digitales, sin embargo, los más usados son el enmascaramiento y filtrado a través de marcas de agua en imágenes, el uso de algoritmos y funciones matemáticas y la inserción de información en el bit menos significativo de cada pixel de una imagen.

Con lo anterior se puede observar que la esteganografía se ha usado desde hace muchos años, incluso ha sido usada por agencias militares, la policía, criminales e incluso civiles.

Estegoanálisis

El estegoanálisis se define como la disciplina que se encarga de detectar la información oculta en un esteganograma, teniendo poco o mucho conocimiento de la técnica esteganográfica que se haya usado.

En el estegoanálisis manual se tienen que buscar manualmente las diferencias entre el contenedor y el esteganograma, la desventaja de este método es que se necesita el contenedor para buscar esas diferencias, si no se tiene, se deben buscar irregularidades en el esteganograma para buscar señales que indiquen que existe información oculta, otra de las desventajas que se tiene es que es posible detectar que hay información oculta, pero no es posible recuperarla.

El estegoanálisis estadístico consiste en hacer un análisis estadístico del esteganograma para encontrar las irregularidades que muestren que se ha ocultado información, por ejemplo, en las imágenes se estudia la frecuencia de distribución de colores.

La esteganografía ha evolucionado considerablemente con el paso del tiempo, tanto que se ha adaptado a las nuevas tecnologías por lo que actualmente hay técnicas muy avanzadas que hacen que el estegoanálisis sea más complejo.

(Velasco Bautista et al., 2007)

3.6.4. Nuevos métodos

La información personal es algo con lo que debe tenerse mucho cuidado, no hay que olvidar lo importante que es mantener segura este tipo de información, para que personas mal intencionadas no hagan mal uso de esta y afecten a las víctimas de diferentes maneras.

Adicionalmente, los datos almacenados en historiales médicos pueden ser usados para realizar investigaciones y con los datos que almacenan los bancos se puede realizar un análisis financiero, situaciones de las cuales muchas veces los dueños de la información no están enterados y no mantienen el anonimato necesario para realizar este tipo de estudios o investigaciones.

Teniendo esto en cuenta, investigadores de la Universidad Rovira y Virgili conocida como UVR o Universitat Rovira i Virgili y de la Universidad Abierta de Cataluña conocida por sus siglas como UOC que significa Universitat Oberta de Catalunya, diseñaron un sistema que es capaz de detectar y ocultar la información confidencial de documentos, dicho trabajo hasta el año 2017 se tenía implementado como un prototipo en software con el cual se habían realizado pruebas con casos clínicos en inglés, cabe mencionar que esta investigación está enmarcada en el proyecto europeo CLARUS, el cual trata sobre la privacidad de datos en la nube, coordinado por la URV, también forma parte del proyecto SmartGlacis tecnologías de seguridad y privacidad para ciudades inteligentes de la UOC.

(Universidad Oberta de Catalunya, 2017)

3.7. Mecanismos de seguridad

3.7.1. Definición y objetivos

Los mecanismos de seguridad son técnicas que pueden funcionar por si solas o en conjunto para implementar servicios de seguridad. Para mantener protegido un sistema debe de realizarse un análisis de las amenazas potenciales que puedan ocurrir, con este análisis se diseñan políticas de seguridad cuyo propósito es evitar las amenazas o disminuir su impacto en caso de llegarse a producir, por lo que un mecanismo de seguridad es el mecanismo con el cual se implementan las políticas de seguridad mencionadas.

Si los mecanismos de seguridad implementados no están configurados adecuadamente, pueden ser usados para provocar un ataque, también pueden realizarse ataques explotando vulnerabilidades no descubiertas o con los propios errores del sistema, de aquí surge la importancia de realizar un buen análisis para configurar los mecanismos de seguridad de acuerdo con lo definido en las políticas.

3.7.2. Tipos de mecanismos de seguridad

Los mecanismos de seguridad se clasifican en mecanismos preventivos, mecanismos de detección y mecanismos de recuperación.

3.7.2.1. Mecanismos de prevención

Aumentan la seguridad del sistema previniendo que ocurran violaciones a la seguridad, es decir, previenen que ocurran amenazas a la triada CID. Dentro de los mecanismos de prevención se encuentran:

- **Mecanismos de autenticación e identificación:** estos identifican a usuarios, sistemas y procesos de manera única, para después con un método de autenticación puedan comprobar que dicho usuario, sistema o proceso es quien dice ser, por lo que este tipo de mecanismos son los más importantes de cualquier sistema.
- **Mecanismos de control de acceso:** el control de acceso es el proceso que permite a un usuario, sistema o proceso tener acceso a partes específicas del sistema. Los administradores pueden restringir el acceso a ciertas partes del sistema para proporcionar mayor seguridad como:
    - Evitar que se haga un uso incorrecto de los recursos.
    - Permitir que los usuarios tengan acceso desde diferentes ubicaciones.

- Permitir el acceso necesario de acuerdo al nivel de privilegios que tengan los diferentes usuarios.
- Identificar y resolver problemas de acceso de manera remota.

(Romero Castro et al., 2018)

3.7.2.2. Mecanismos de detección

Este tipo de mecanismo detecta las violaciones o intentos de violación a la seguridad del sistema. Uno de los sistemas más usados para reducir el riesgo de ocurrencia de un ataque dirigido son los IDS.

Un IDS supervisa los componentes que forman la red, de igual manera monitorea a los usuarios, sistemas y procesos que quieren acceder de manera ilegal al sistema y describe la actividad que realizan sobre los elementos de la red.

Los componentes de un IDS son:

- **Sensores:** coleccionan la información y la envían a los analizadores.
- **Analizadores:** determinan si está ocurriendo una intrusión, en caso de que sí esté ocurriendo presentan una serie de pruebas, entre ellas el tipo de intrusión detectada y después, dependiendo del IDS se ejecutan medidas para actuar en contra de la intrusión.

(Romero Castro et al., 2018)

3.7.2.3. Mecanismos de recuperación

Estos mecanismos son los que se llevan a cabo cuando ocurrió una violación a la seguridad del sistema y tras detectarla, el administrador del sistema debe de recuperarlo para que el sistema vuelva a funcionar de manera normal.

El objetivo de los backups o copias de seguridad es crear una copia de los datos para que estos puedan ser restaurados en caso de ser necesario, estos backups solo son una parte del plan de protección contra desastres, por lo que es necesario realizar un buen trabajo para que proporcione un nivel de recuperación de datos adecuado.

Para realizar una copia de seguridad, el administrador debe de seguir las políticas de seguridad de la empresa u organización, y debe considerar lo siguiente:

- Es importante que tenga muy claro qué es lo que debe copiar, para esto debe alinearse con las políticas de seguridad de la organización.
- También debe tener estipulado quién será la persona encargada de realizar las copias y en que dispositivo se estarán realizando.

- Además de lo anterior, deben considerarse las condiciones bajo las cuales se realizarán las copias de seguridad y la frecuencia con la que se harán para cubrir las necesidades de recuperación de la organización.

(Romero Castro et al., 2018)

Tema 4. Políticas de seguridad informática dentro de la organización

4.1. Políticas de seguridad informática

4.1.1 Objetivo de una política de seguridad

Las políticas de seguridad son reglas que definen qué se quiere proteger y qué es lo que se espera de los usuarios, es decir, se describen las acciones necesarias que debe llevar a cabo el usuario para proteger el recurso para el cual se están creando dichas políticas.

Para desarrollar de manera efectiva las políticas de seguridad, se deben de definir los objetivos de seguridad, y después de que se crean deben de ponerse en práctica, dentro de esto se incluye la capacitación de los empleados y/o personas que tengan permitido el acceso al recurso en cuestión, además de añadir el hardware y software necesario para seguir las políticas adecuadamente.

En el siguiente listado se muestran algunos de los objetivos de las políticas de seguridad:

- **Protección de recursos:** este hace referencia a que únicamente usuarios con autorización tienen permitido acceder a los recursos.
- **Autenticación:** es la parte de seguridad que verifica la identidad del proceso, sistema o usuario que quiere acceder al recurso. Los métodos de autenticación tradicionales incluyen el uso de nombres de usuario y contraseñas, sin embargo, actualmente los certificados o firmas digitales proporcionan un método más seguro de autenticación.
- **Autorización:** a través de éste se determina si el proceso, sistema o usuario que quiere acceder al recurso tiene los permisos necesarios para realizar la petición que está haciendo.
- **Integridad:** permite asegurar que la información que recibe el receptor es la misma que fue enviada por el emisor, es decir, la integridad se asegura de que la información no ha sido modificada en el trayecto a su destino.
- **Confidencialidad:** hace referencia a que la información solo es visible para usuarios, sistemas o procesos autorizados. La confidencialidad es un punto importante para la seguridad total de la información.

Las políticas deben crearse de acuerdo a las necesidades de cada organización, además de mostrar el compromiso de los altos cargos para hacer cumplir dichas políticas. Una buena práctica es definir a un responsable, quien debe comunicar continuamente a todas las partes interesadas las políticas y sus actualizaciones.

(Bustamante Sánchez, s. f.; Fidetia, 2015; IBM, 2023)

4.1.2. Misión y visión de la organización

La misión y visión de una organización son bastante útiles, ayudan a establecer un camino para que la organización alcance el éxito, además, permiten definir los objetivos que se quieren alcanzar a corto, mediano y largo plazo, en otras palabras, la misión y la visión describen la identidad de una organización.

La misión describe la razón de ser de la organización, es decir, el motivo por el que la organización existe y tiene relación con el presente, regularmente responde a preguntas como ¿Quiénes son? y ¿A qué se dedica la organización? Así, es importante que la misión resalte la diferencia que hay con las organizaciones similares en el mercado para mostrar un valor único, también debe reflejar las necesidades que intenta satisfacer y los beneficios que los usuarios tendrán si cuentan con los productos o servicios que ofrecen.

Una misión debe ser:

- Corta, precisa y fácil de comprender.
- Motivadora, para que los empleados se sientan incentivados y busquen alcanzar las metas propuestas.
- Original, para que se diferencie de las organizaciones similares en el mercado.

La visión describe las metas y los propósitos que la organización quiere alcanzar en un futuro, asimismo, describe los medios que usará para lograrlo, ésta puede cambiar con el paso del tiempo, sin embargo, deben de conservarse los valores con los cuales la organización fue creada. La visión responde a preguntas como ¿Qué se desea lograr? o ¿Hacia dónde se dirige la organización?

La visión debe:

- Proyectarse a corto, mediano y largo plazo.
- Ser realista, es decir, que puedan alcanzar los objetivos propuestos.
- Ser clara, para que todos puedan comprenderla.

Adicionalmente se tienen los valores, estos son principios sobre los cuales se fundamentan las acciones y decisiones que se toman en la organización, los valores complementan la visión y misión, por lo que deben ser coherentes entre sí.

Los valores hacen referencia al comportamiento ético de la empresa, responde a preguntas como ¿En qué cree la organización? o ¿Cómo es su cultura organizativa?, se podría decir que describen la personalidad de la empresa.

La misión, visión y valores son muy importantes porque permiten definir la estructura, objetivos, forma de actuar o la importancia de la organización en la sociedad, por lo que se dice que estos

tres conceptos son los pilares sobre los cuales se sostienen las organizaciones, porque permiten mantener su identidad a lo largo del tiempo.

(Crecer, 2018; Santander Universidades, 2022; UNIR México, 2022)

4.1.3. Principios fundamentales de las políticas de seguridad

Las políticas de seguridad deben de garantizar en todo momento confidencialidad, integridad y disponibilidad de los activos que protegen, asimismo, deben de prevenir y reducir los riesgos.

Las políticas de seguridad deben definir los siguientes aspectos:

- Se debe establecer quienes pueden usar los recursos, a cada uno de los empleados se les asigna el uso de los recursos de acuerdo a sus necesidades.
- Se deben establecer pautas que definan claramente cuál es el uso aceptable de los recursos.
- Se debe de elegir al usuario que tendrá los privilegios de administrador, este será el responsable de cuidar que se cumplan las políticas de seguridad.
- Se debe elegir un responsable que esté pendiente de las actualizaciones que se requieran en las políticas de seguridad.
- Se deben definir los derechos y las responsabilidades de los usuarios, dentro de esto se incluye la implementación de acciones legales si algún usuario hace un uso inaceptable de los recursos que ponga en riesgo a los activos que protegen las políticas.

Adicionalmente se debe seguir una metodología para crear correctamente políticas de seguridad:

1. **Definición de objetivos:** es decir, identificar porqué es necesaria la política que se quiere definir, también es necesario tomar en cuenta el entorno del sistema para desarrollar las políticas de manera adecuada.
2. **Preparación:** hay que realizar un análisis de los activos que se quieren proteger, durante este análisis se tiene que determinar que recursos se van a proteger y como es que se quieren proteger, asimismo se debe de realizar un procedimiento donde se estime el riesgo de los activos y su pérdida.
3. **Redacción de políticas:** se debe tener clara la forma en la que se van a redactar las políticas, es decir, si se van a redactar de forma permisiva o prohibitiva, además deben estar escritas en tiempo presente y debe de considerarse el entorno del sistema. En la redacción deberán definirse sanciones que se llevarán a cabo si es que alguno de los usuarios viola alguna de las políticas de seguridad, ya que esto puede provocar que todo el sistema se ponga en riesgo.

Las políticas permisivas son aquellas en las que todo está permitido a excepción de lo que está explícitamente prohibido, mientras que las políticas prohibitivas son aquellas en las todo está prohibido a excepción de aquello que está explícitamente permitido.

4. **Aprobación de las políticas:** después de haber sido redactadas, las políticas deberán enviarse a los directivos, quienes deberán dar su aprobación o en caso de ser necesario deberán hacer los cambios correspondientes para obtener la versión final de las políticas.
5. **Difusión de las políticas:** después de que las políticas son aprobadas por los directivos de TI, deben de difundirse a los usuarios para que empiecen a aplicarlas, en caso de ser necesario, los usuarios deberán recibir capacitaciones, con la finalidad de que aprendan a aplicar correctamente dichas políticas.

La seguridad es un ciclo que continuamente debe estar mejorando y las políticas de seguridad no son la excepción, la creación de políticas también es un ciclo, por lo que después de ser difundidas pueden mantenerse o actualizarse, esto dependerá de diferentes factores entre los cuales se encuentran:

- Nuevos riesgos identificados.
- Violación de alguna de las políticas.
- Sugerencias de las partes interesadas.
- Cambios importantes dentro de la organización.

Durante el desarrollo de las políticas también debe de tomarse en cuenta que hay diferentes tipos de participantes involucrados y cada uno de ellos tiene un rol muy importante durante el desarrollo de las mismas:

- **Administradores de sistemas:** son los encargados de monitorear que las políticas se cumplan correctamente y se mantengan en constante actualización, asimismo deben de mantener actualizada la información de los usuarios para eliminar las cuentas o datos de usuarios que ya no laboren en la organización, también son los encargados de vigilar que el sistema trabaje de manera eficiente.
- **Personas con autoridad:** son los encargados de aprobar las políticas de seguridad antes de que sean difundidas a los usuarios, también deben asegurarse de que estén implementadas correctamente y cubran las necesidades de la organización.
- **Representante jurídico:** es el encargado de llevar a cabo las sanciones correspondientes con los usuarios que hayan violado las políticas de seguridad, ya que puede haber situaciones en donde el tipo de violación requiera que la organización tome acciones legales.
- **Editor o redactor:** es una persona o grupo de personas que se encargan de redactar las políticas de seguridad y editarlas cuando sea necesario.
- **Usuarios:** es el grupo de personas que deberá llevar a la práctica las políticas de seguridad implementadas.

Las políticas de seguridad son fundamentales para las organizaciones, ya que estas ayudarán a los usuarios a mantener los sistemas seguros siguiendo una serie de pautas, cumpliendo así los objetivos de seguridad de una organización.

(Bustamante Sánchez, s. f.; Fortra, 2018; Mendoza, 2014b; Pirani, s. f.-a)

4.1.4. Modelos de seguridad

Un modelo de seguridad es un esquema donde de manera formal se presentan las políticas de seguridad, este tiene que describir las reglas y prácticas que indican cómo un sistema debe manejar, proteger y distribuir la información, asimismo, deben de identificar los riesgos para implementar acciones que ayuden a reducir su impacto.

Los objetivos de un modelo de seguridad son:

- Validar la identidad de los usuarios del sistema, esto se logra mediante métodos de autenticación.
- Garantizar la integridad de los datos.
- Garantizar que la información confidencial sea protegida.
- Validar que los usuarios tengan el acceso a los recursos necesarios de acuerdo a su nivel de privilegios en el sistema.

Tipos de modelos de seguridad

Modelos de control de acceso

Estos modelos identifican reglas que aseguran que el acceso que se tiene a los recursos está previamente autorizado, es decir, este tipo de modelos de seguridad protegen la confidencialidad y la integridad. Algunos de estos modelos de seguridad son:

- **Matriz de control de acceso:** fue propuesta por Butler W. Lampson en el año 1971, ésta es una herramienta que ayuda a gestionar el acceso que tienen los empleados a la información o activos dentro de una organización.
  Las matrices de control de acceso pueden ser usadas como un modelo de permisos estáticos a los sistemas.
  Este modelo de seguridad cuenta son los siguientes elementos:
  - **Objeto:** se refiere a los activos que se van a proteger.
  - **Sujeto:** hace referencia a la entidad que accede a los objetos, un sujeto puede ser un usuario, un proceso o un programa.
  - **Derecho de acceso:** se refiere a la forma en la que un sujeto accederá a un objeto, estos derechos de acceso pueden ser lectura, escritura, ejecución u otro permiso que se crea necesario o que se pueda realizar sobre los objetos.

Una matriz de acceso puede ser descrita como una matriz en donde las filas son los sujetos y las columnas son los objetos, y en las celdas se indica el modo de acceso que tiene el sujeto con los diferentes objetos, tal como se muestra en la tabla 4.1

Tabla 4.1. Matriz de control de acceso.

	Objetos			
Sujetos		**Objeto 1**	**Objeto 2**	**Objeto 3**
	Usuario 1	*Escritura*	*Lectura*	*Escritura*
	Proceso 1	*Ejecución*	*Lectura*	*Lectura*
	Programa 1	*Escritura*	*Lectura*	*Ejecución*

Este tipo de matrices son muy útiles ya que muestran claramente el tipo de acceso que tienen los sujetos a los objetos, por lo que tener una matriz de control de acceso es una práctica recomendable más no obligatoria para cumplir con las normas de seguridad de la norma ISO 27001.
(Ballesteros Riveros & Calas Sierra, 2007; Bustamante Sánchez, s. f.; UNAM, s. f.-a)

- **Modelo de Bell-LaPadula:** este modelo de seguridad fue definido entre los años 1973 y 1976 por David Elliott Bell y Len LaPadula. El propósito inicial de su desarrollo fue para cumplir con requerimientos de acceso a la información del DOD de EE.UU, este modelo está enfocado exclusivamente en proteger la confidencialidad de la información.
  El modelo Bell-LaPadula divide a los sistemas de información en sujetos y objetos, donde los sujetos son los usuarios o los procesos que ejecuta un usuario, mientras que los objetos son los recursos a los cuales se les va a controlar el acceso.
  Para proteger el acceso a los objetos se tienen que implementar reglas de control de acceso, las cuales le van a permitir a los sujetos leer los objetos de su nivel o de niveles inferiores, asimismo, los sujetos pueden participar en la creación de objetos de su mismo nivel o de niveles superiores.
  Los niveles de seguridad de este modelo se clasifican en:
  - Alto secreto.
  - Secreto.
  - Confidencial.
  - No clasificado.

  Donde, el nivel más alto es el de alto secreto y el nivel más bajo es el nivel no clasificado, de igual manera, se usan estas clasificaciones de seguridad para aceptar o denegar las solicitudes hechas por los usuarios.
  El modelo de Bell-LaPadula es un modelo que puede ser aplicado en sistemas operativos y bases de datos.
  En la tabla 4.2 se muestra un ejemplo de este modelo:

Tabla 4.2. Modelo de Bell LaPadula.

Clasificación de seguridad	Sujeto	Objeto
Alto secreto	Sujeto A	Objeto 1
Secreto	Sujeto B	Objeto 2
Confidencial	Sujeto C	Objeto 3
No clasificado	Sujeto D	Objeto 4

En la tabla 4.2 se muestran las clasificaciones de seguridad de este modelo, así como los objetos a los que puede acceder cada uno de los sujetos. Las reglas de control de acceso que describe este modelo pueden entenderse de la siguiente manera:

- El sujeto A tiene permitido leer los objetos 1, 2, 3 y 4, pero únicamente puede crear y escribir objetos que tengan la clasificación de alto secreto.
- El sujeto B tiene permitido leer los objetos 2, 3 y 4, además puede crear y escribir objetos cuya clasificación sea secreto y alto secreto.
- El sujeto C tiene permitido leer los objetos 3 y 4, además de escribir y crear objetos cuya clasificación sea: confidencial, secreto y alto secreto.
- El sujeto D solo tiene permitido leer el objeto 4, sin embargo, puede escribir y crear objetos con clasificaciones de seguridad: no clasificado, confidencial, secreto y alto secreto.

Dicho de otra manera, la lectura se hace desde el nivel asignado hacia los niveles inferiores, mientras que la creación y escritura se hacen en el mismo nivel o en niveles superiores.

(Ballesteros Riveros & Calas Sierra, 2007; Bustamante Sánchez, s. f., s. f.; CCN CERT, s. f.-c)

- **Modelo Harrison-Ruzzo-Ullman:** el modelo de Harrison-Ruzzo-Ullman o HRU fue propuesto en el año 1976 por Michael Harrison, Walter Ruzzo y Jeffrey Ullman, quienes con este modelo intentaron mejorar la matriz de control de acceso, esto debido a que la matriz carece de seguridad.

  El modelo HRU es un modelo de control de acceso discrecional, sus componentes son:

  - Un conjunto de sujetos, denominado como S.
  - Un conjunto de objetos denominado como O.
  - Un conjunto de permisos de acceso, denominado R.
  - Una matriz de control de acceso denominada como M.

Adicionalmente, el modelo HRU tiene seis operaciones primitivas con las cuales se puede manipular el conjunto de sujetos, objetos y la matriz de acceso:

- **Create subject S:** le permite a un sujeto agregar un nuevo sujeto S a un sistema.

- **Create object O:** esta operación le permite a un sujeto agregar un nuevo objeto O al sistema.
- **Delete subject S:** el controlador del sujeto S le permite eliminar al sujeto S del sistema.
- **Delete object O:** le permite al propietario del objeto eliminar al objeto O del sistema.
- **Enter R into M_{so}:** con esta operación, el propietario del objeto O le puede asignar derechos R al sujeto S.
- **Delete R from M_{so}:** le permite al propietario de un objeto O eliminar algún derecho R que tenga el sujeto S sobre el objeto O.

El funcionamiento del modelo HRU puede observarse en la figura 4.1:

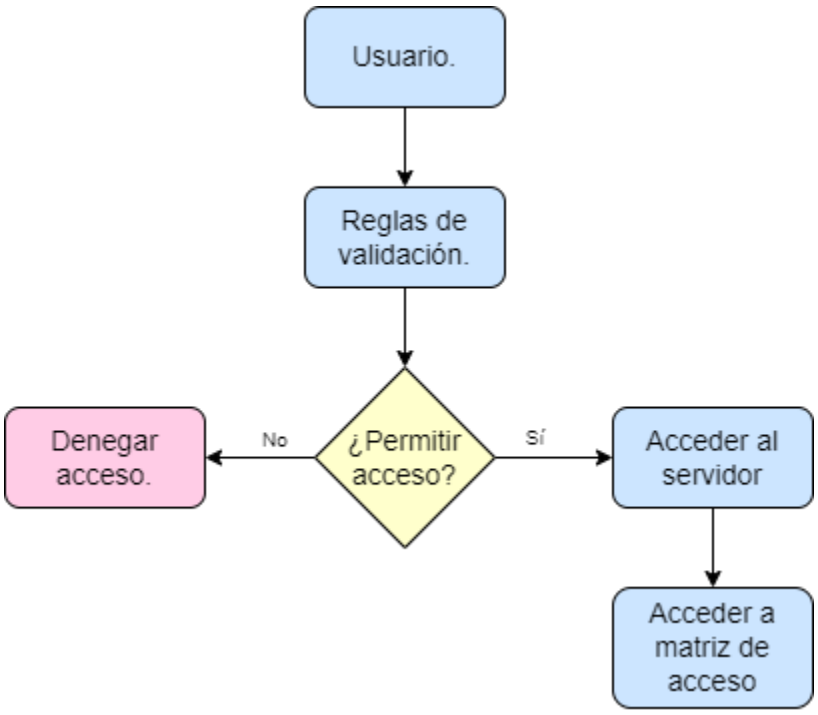


Figura 4.1. Funcionamiento del modelo HRU.

De acuerdo con la figura 4.1, el usuario se encarga de realizar una petición para acceder al servidor, esta petición pasa por las reglas de validación, las cuales verifican si el usuario cumple los requisitos para tener acceso al servidor, si cumple dichos requisitos, se le permite ingresar al servidor, y por consiguiente podrá acceder a la matriz de acceso, pero, si no cumple con los requisitos se le deniega el acceso al servidor.

Este modelo al estar basado en la matriz de control de acceso solamente se preocupa por la confidencialidad de los objetos del sistema, sin tener en cuenta la integridad y la disponibilidad de los datos.

(Alturi, 2011; UNAM, s. f.-a)

Modelos de integridad

Este tipo de modelos tienen como objetivo conservar la consistencia interna y externa de los datos, así como prevenir las modificaciones no autorizadas, es decir, protegen la integridad. Los dos tipos de modelos de integridad son:

- **Modelo Clark Wilson:** este modelo de seguridad fue desarrollado entre los años 1987 y 1989 por David D. Clark y David R. Wilson, está diseñado para entornos comerciales, este modelo busca evitar que los datos se modifiquen sin autorización.
  Las políticas de integridad de este modelo son:
  - **Transacciones correctas:** esta política se refiere a que los usuarios puedan realizar modificaciones a los datos en situaciones específicas, evitando así que se realicen modificaciones incorrectas.
  - **Separación de obligaciones:** esto hace referencia a que las operaciones que puede realizar un usuario tienen que ser acordes al nivel de su perfil.

  Asimismo, cuenta con dos grupos de datos:
  - **Elementos de datos restringidos o CDIs:** elementos de los cuales debe preservarse la integridad.
  - **Elementos de datos no restringidos o UDIs:** elementos que no están protegidos con las políticas de integridad.

  También hay dos tipos de procedimientos que ayudan a conservar la consistencia de los datos:
  - **Procedimientos de verificación de integridad o IVP:** tienen como objetivo validar que los CDI se encuentren válidos.
  - **Procedimientos de transformación o TP:** hacen referencia a las operaciones que manipulan los CDI, es decir, los pasan de un estado válido a otro estado que también sea válido. Los únicos que pueden manipular a los CDIs son los TP, por lo que el sistema debe asegurarse de que esto se cumpla.

  Adicionalmente se aplican nueve reglas para alcanzar la integridad:
  - **Reglas de certificación:** son ejecutadas por el administrador, las decisiones se toman hasta que alguna automatización sea posible.
    - **C1 – certificación IVP:** los IVP tienen que asegurar que los CDI estén en un estado válido cuando el IVP está en ejecución.
    - **C2 – Validez:** los TPs llevan a un CDI a un estado final, el cual debe ser válido.
    - **C3:** la lista de relaciones E2 (ejecución de separación de obligaciones) debe estar certificada.
    - **C4 – certificación de bitácora:** los TPs tienen que contar con una certificación para contar con acceso de entrada
    - **C5:** los TP que transforman UDIs a CDI deben estar certificados.

- **Reglas de ejecución:** se implementan en el sistema, por lo que el sistema es el que las garantiza.
  - **E1 – ejecución de validez:** el sistema debe asegurar que las manipulaciones a los CDI sean realizadas mediante un TP.
  - **E2 – ejecución de separación de obligaciones:** el sistema debe tener una lista donde se relacione al usuario, al TP y a los CDI que deben ser manipulados por el TP.
  - **E3 – identidad del usuario:** los usuarios que llaman a los TPs deben pasar por un proceso de autenticación.
  - **E4 – iniciación:** únicamente algunos usuarios deben de especificar las relaciones.

En la figura 4.2, se observa el contenido de este modelo a grandes ragos.

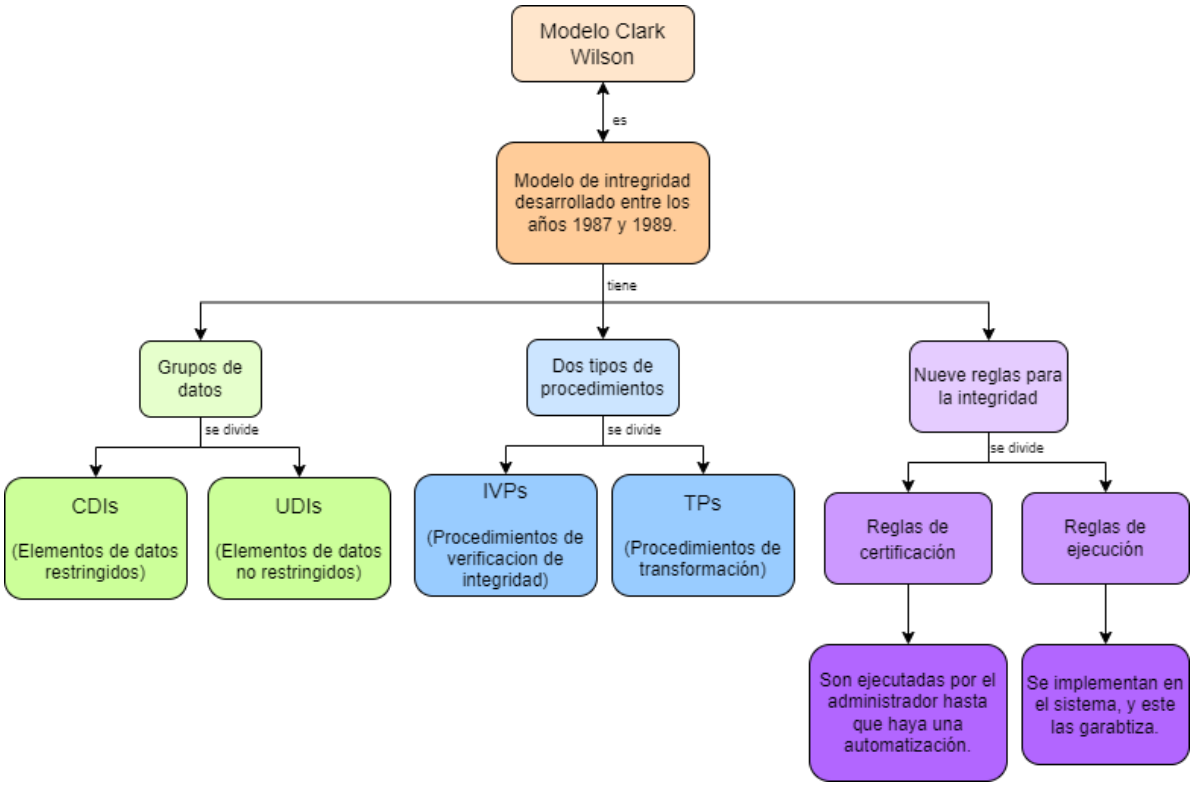


Figura 4.2. Modelo Clark Wilson.

Un ejemplo de la aplicación de este modelo es el siguiente:
En una tienda, un empleado está a cargo de realizar la compra de los productos faltantes, por lo que hace una lista de dichos productos la cual envía al proveedor y a la persona que recibirá los productos cuando lleguen, es decir, al encargado de recepción.
Cuando llegan a la tienda los productos, son recibidos por el encargado de recepción, quien, al momento de recibirlos, verifica los productos con la lista que le envió el empleado, al verificar que está recibiendo correctamente lo que se le pidió al proveedor

firma la orden de recibido y envía dicha orden junto con la lista original al dueño de la tienda, ya que es quién pagará al proveedor.

El proveedor envía al dueño de la tienda la factura con el costo total de los productos, el dueño al recibirla, la comparara con la orden de recibido y la lista original que le envió el encargado de recepción, y al verificar que todo es correcto, envía al proveedor un cheque pagándole el total de los productos.

En el ejemplo anterior, los TP son todos los procedimientos que hacen que se mantenga la integridad de la información, es decir, crear la lista de productos, enviarla al proveedor y al encargado de recepción, la creación y firma de recibido, el envío de la factura y la comparación que hace el dueño de la tienda antes de emitir el cheque de pago. Los usuarios son el empleado encargado de realizar la compra de productos, el proveedor, el encargado de recepción y el dueño de la tienda. Y los CDI son la lista de productos, la orden de recibido, la factura y el cheque.

Con este modelo se puede comprender que las funciones de cada una de las áreas dentro de una organización no pueden ser ejecutadas por un área diferente, porque se perdería la integridad de la información, por eso es importante que haya personas especializadas en cada una de las áreas para que la información sea tratada correctamente por expertos lo que evitaría que la información sea manejada por personal con poca o nula experiencia en el área, y así la organización mantiene la integridad de la información.

(Bustamante Sánchez, s. f.; Herrera et al., 2012)

- **Modelo Biba:** este modelo fue propuesto por Kenneth J. Biba en el año 1977, describe reglas de control de acceso las cuales están enfocadas a mantener la integridad de los datos, basándose en los siguientes objetivos:
    - Anticipar la modificación de los datos por usuarios o procesos no autorizados.
    - Prevenir que se realice la modificación de datos no autorizados por usuarios o procesos sin autorización.
    - Mantener la consistencia interna y externamente.

  En este modelo, los usuarios y procesos solo pueden crear objetos en su propio nivel y en niveles inferiores, también, pueden leer la información que se encuentra en su mismo nivel o en niveles superiores, pero no pueden leer la información que se encuentra en niveles inferiores, ya que, de acuerdo con este modelo, la integridad de la información se pone en riesgo.

En la tabla 4.3 se muestra un ejemplo de este modelo:

Tabla 4.3. Modelo Biba.

Nivel de seguridad	Usuario/Proceso	Objeto
Alto	Usuario A	Objeto 1
Medio	Proceso 1	Objeto 2
Bajo	Proceso 2	Objeto 3

Tomando en cuenta la información de la tabla 4.3 el funcionamiento de este modelo es el siguiente.

- El usuario A puede crear objetos en todos los niveles de seguridad, sin embargo, solo puede leer la información que tenga un alto nivel de seguridad.
- El proceso 1 solo puede crear objetos con un nivel de seguridad medio o bajo, y puede leer información que tenga un nivel de seguridad medio y alto.
- El proceso 2 solo puede crear objetos con un nivel de seguridad bajo, y puede leer información que tenga un nivel de seguridad bajo, medio o alto.

Un ejemplo de este modelo es que un estudiante puede leer un libro escrito por su profesor, sin embargo, no puede crear materiales de estudio para el profesor, puede crearlos solo para él. En cambio, el profesor si puede crear materiales de estudio para el alumno y el alumno puede usarlos, pero el profesor no puede leer un libro desarrollado por su alumno.
(Carrillo Jiu, 2014; López Barrientos & Quezada Reyes, 2019)

4.1.5. Desarrollo de políticas orientadas a servicios de seguridad

Las políticas de seguridad definen pautas para proteger la información, adicionalmente hay que dejar claro cual es el rol de cada miembro, las excepciones y consecuencias que puede haber por incumplir alguna de las políticas de seguridad.

De acuerdo con la norma ISO 27000, las políticas de seguridad deben:

- Ser compatibles con otras políticas.
- Contar con una persona que se haga responsable de mantenerlas y actualizarlas.
- Ser de fácil acceso para que todos los usuarios puedan ponerlas en práctica adecuadamente.

Para que las políticas de seguridad sean efectivas deben considerarse las necesidades específicas de la organización, como el sector, estructura, tamaño, entre otros aspectos,

asimismo deben tenerse en cuenta los objetivos de negocio y la alta dirección debe de mostrar compromiso con el cumplimiento de las políticas.

Para desarrollar una política de seguridad deben de seguirse los siguientes pasos:

- **Definición de la política:** puede verse como una descripción general del para que está siendo creada la política.
- **Definición de objetivo:** se debe especificar el objetivo principal de la política, este objetivo debe estar alineado con los objetivos de la organización.
- **Definición del alcance de la política:** esto hace referencia a áreas, procesos, actividades, activos y personas a las que aplica, estos aspectos son clave, ya que se deben tener en cuenta para el cumplimiento de la política.
- **Establecimiento de roles y responsabilidades:** como lo indica la norma ISO 27001, en las políticas de seguridad deben de indicarse los roles para la implementación, seguimiento y autorizaciones de las políticas, asimismo se deben definir las responsabilidades de los usuarios, esto ayuda a garantizar que las políticas de seguridad se cumplan.
- **Especificación de las reglas de aplicación:** esto hace referencia a los aspectos que deben de cumplir de manera obligatoria los usuarios. También se incluyen las reglas que ayudarán a preservar la seguridad de la información, por ejemplo, reglas relacionadas con la administración de claves, o gestión de los respaldos de información.
- **Definición de sanciones:** estas sanciones se aplicarán cuando se incumpla alguna de las políticas, dichas sanciones van desde llamadas de atención, anulación o suspensión de permisos hasta denuncias legales.
- **Revisión de la política:** después de que la política fue redactada, debe ser evaluada por expertos, quienes sugerirán los cambios pertinentes para la creación, modificación o actualización de las políticas.
- **Desarrollo de glosario:** se debe de incluir un glosario de términos para que todos los usuarios entiendan de manera clara las políticas y no haya confusiones en su aplicación.
- **Aprobación de la política:** la alta dirección o una persona encargada deberá formalizar dicha política de seguridad, esto se hará mediante la firma y publicación de la política.

Se debe incluir un apartado que tenga información como por quién fue elaborada la política, la versión, la fecha de actualización, y los nombres de quien revisó y quien aprobó la política, de igual manera las políticas deben de monitorearse para verificar que se estén cumpliendo correctamente.

Después de que las políticas son publicadas para que los usuarios las lleven a cabo, se debe de especificar cada cuanto tiempo se deberán realizar las revisiones y actualizaciones correspondientes, lo recomendable es realizarlas como mínimo una vez al año.

Es importante mencionar que, si hay cambios en el entorno del sistema o en el sistema mismo, las políticas de seguridad deben de actualizarse para que cubran las nuevas necesidades de la organización.

Finalmente, puede haber una etapa de retiro, en donde las políticas se eliminan por completo, ya sea porque cumplieron con su propósito o porque dichas políticas ya no son necesarias.

(López Barrientos & Quezada Reyes, 2019; MINTIC, 2016)

4.1.6. Publicación y difusión de las políticas de seguridad

La difusión de las políticas de seguridad es indispensable, en esta etapa los encargados divulgan las políticas, así como los objetivos, metas y beneficios que se van a obtener, el propósito de la difusión es que los usuarios correspondientes conozcan las políticas y creen conciencia de su importancia para que las lleven a cabo correctamente, asimismo, deben de difundirse las modificaciones que se realicen, dicha difusión puede llevarse a cabo empleando diferentes métodos o herramientas, las cuales garanticen que las políticas lleguen a los usuarios correspondientes. Entre estos métodos y herramientas se encuentran:

- **Manuales de empleado:** incluyen toda la información relacionada con la organización, como la misión, visión, valores, historia, entre otra información. Una opción de difusión es incluir las políticas de seguridad en los manuales de empleado, así las conocen desde que incorporan a la organización.
- **Boletines informativos:** el propósito de los boletines informativos es hacer llegar a los empleados información importante, en estos se pueden incluir las políticas de seguridad, así como las modificaciones que se lleguen a realizar.
- **Circulares:** estos son documentos formales usados por autoridades para dar a conocer información a una población en específico, por lo que una buena opción es incluir en las circulares las políticas de seguridad y las modificaciones que se realicen.
- **Correos electrónicos:** esto también suele ser muy útil, ya que en muchas organizaciones el correo electrónico es el medio de comunicación principal que tienen los altos mandos con los demás empleados.
- **Intranet:** la intranet es la red de comunicación interna de la organización, a través de ella podrían difundirse las políticas de seguridad. Al hacer la difusión de las nuevas políticas, cambios, actualizaciones y sanciones es importante que se tenga una sección donde los usuarios encuentren toda esta información rápidamente, asimismo, se deberán de enviar avisos a los usuarios indicando que hubo cambios e informándoles donde podrán encontrar la información actualizada.

Con algunos de los cambios implementados o con el surgimiento de nuevas políticas es probable que los usuarios necesiten ser capacitados, esto se debe a que es posible que no

todos los usuarios tengan el suficiente conocimiento para adecuarse a las políticas, por lo que las capacitaciones también deben de tenerse en cuenta.

Siempre que se difundan las nuevas políticas de seguridad o actualizaciones sobre políticas existentes, es importante hacer saber a los usuarios el motivo del surgimiento de las nuevas políticas o porqué se están realizando las actualizaciones o cambios, esto brindará a los usuarios claridad acerca del porque se están tomando ciertas acciones y podrán emplearlas de una manera eficiente, también al difundir las políticas se deben difundir las sanciones que se tomaran en caso de que alguien no cumpla las políticas de seguridad establecidas.

De ser necesario hay que organizar reuniones donde los altos mandos expliquen las nuevas políticas, actualizaciones, cambios, así como las sanciones correspondientes, con la finalidad de que todo quede mucho más claro y no haya lugar para dudas o malentendidos.

(Tovar, 2022)

4.2. Procedimientos y planes de contingencia

4.2.1. Procedimientos preventivos

El mantenimiento preventivo es aquel que consiste en hacer revisiones en el hardware o software de un sistema, con la finalidad de detectar fallos que puedan generar problemas que afecten el rendimiento del sistema.

Para realizar un buen mantenimiento preventivo debe planearse cuidadosamente, esto porque muchas veces será necesario detener las actividades del sistema por completo para que cada uno de los dispositivos que lo conforman sean analizados y se puedan tomar las medidas necesarias.

Hay dos tipos de mantenimiento preventivo:

- **Basado en tiempo:** se tienen que hacer las revisiones de manera periódica cada cierto tiempo, este tiempo puede ser determinado por un grupo de expertos tomando como base experiencias previas, también podrían usarse métodos estadísticos o modelos matemáticos si se cuenta con la información suficiente.
- **Basado en el uso:** este método se basa en el uso real que se les ha dado a los diferentes dispositivos, por lo que la revisión se realiza tomado en cuenta las horas de funcionamiento efectivas del dispositivo.

Para que el plan de mantenimiento sea efectivo deben definirse las siguientes etapas:

1. **Definir los objetivos:** es decir, definir que se espera al aplicar el mantenimiento, como alargar la vida útil de los dispositivos, detectar posibles fallos para corregirlos y reducir costos al evitar aplicar un mantenimiento correctivo, entre otros.
2. **Inventario de dispositivos:** los dispositivos deberán estar organizados, ya sea por ubicación, función, entre otros, asimismo deben de identificarse los dispositivos que son esenciales para que el sistema funcione adecuadamente, ya que si estos dispositivos llegaran a fallar el funcionamiento del sistema se vería sumamente afectado. También se debe de contar con los manuales y recomendaciones del fabricante de los dispositivos.
3. **Revisión de planes de mantenimiento anteriores:** para tener referencia de tiempos y costos de las implementaciones, si no se tienen planes de mantenimiento anteriores deberá empezarse desde cero, con ayuda de los expertos.
4. **Elección de las tareas a realizar:** para realizar mantenimiento preventivo se pueden llevar a cabo alguna de las siguientes medidas:
    a. **Tareas de mantenimiento:** éstas son las que se realizan para minimizar la ocurrencia de fallas, entre las tareas que se puede realizar se encuentran: inspecciones visuales, limpiezas técnicas, revisión de ajustes, cambio de componentes, entre otros.
    b. **Mejoras y modificaciones:** la ocurrencia de problemas también puede minimizarse si se aplican mejoras o algún tipo de cambio, como cambio de alguno de los componentes que tenga mejores características que cubran las necesidades de la organización, instalación o actualización de software, cambios en la configuración de los dispositivos, entre otros.
    c. **Cambiar los procedimientos operativos:** es posible que se haya detectado que haciendo cambios en la forma de operar el sistema se puedan minimizar los fallos y/o alargar la vida útil de los dispositivos, sin embargo, esto puede ocasionar que se necesite capacitar a los usuarios, lo que genera costos.
5. **Elegir el tipo de mantenimiento preventivo a realizar y a los encargados que lo llevarán a cabo:** esto es importante porque se va a definir la frecuencia de mantenimiento, y si va a ser un mantenimiento basado en el tiempo o en el uso, asimismo se eligen a los responsables para que realicen los mantenimientos de manera periódica.
6. **Entrega de reportes:** después de que el plan de mantenimiento fue realizado con éxito, los responsables deben generar los reportes finales de mantenimiento, ya que estos son importantes para realizar el seguimiento correspondiente.

Realizar un plan de mantenimiento preventivo correctamente va a ser muy útil, ya que ayudará a reducir costos, alargar la vida útil de los dispositivos y evitar que el sistema se detenga en un momento inesperado, lo que a su vez proporcionará una mejor experiencia en la calidad del servicio que se ofrece.

(Emaint., 2021)

4.2.2. Procedimientos correctivos

El mantenimiento correctivo es el tipo de mantenimiento que tiene como objetivo corregir los fallos que se presenten en un sistema para que vuelva a funcionar con normalidad, es decir, este tipo de mantenimiento se realiza después de que algún fallo inesperado interrumpió el funcionamiento del sistema, debe realizarse de manera inmediata, ya que parte del sistema o el sistema completo puede dejar de funcionar, afectando directamente la productividad.

Al contrario del mantenimiento preventivo, el mantenimiento correctivo no tiene una frecuencia establecida para ser llevado a cabo, ya que este se realizará en momentos específicos para restaurar el funcionamiento del sistema.

El procedimiento que se sigue para realizar mantenimiento correctivo va a variar dependiendo de la parte del sistema o dispositivo que falle, sin embargo, el proceso general para realizar mantenimiento correctivo es el siguiente:

1. Después de que el fallo fue detectado debe ser confirmado por los encargados y/o expertos, quienes al confirmar que el sistema ha fallado deberán hacer un informe de fallos antes de tomar las medidas necesarias.
2. Posteriormente se debe localizar el origen del fallo, es decir, se debe localizar el dispositivo especifico que produjo el fallo.
3. Una vez identificado el origen del fallo, hay que hacer un diagnóstico para saber si la parte que falló puede repararse o si es necesario sustituirla.
4. A continuación, hay que hacer pruebas para verificar que el dispositivo arreglado o sustituido responda como es esperado para que el sistema vuelva a funcionar con normalidad.
5. Finalmente, se tienen que realizar pruebas al sistema en conjunto para verificar que esté funcionando correctamente después de haber realizado el mantenimiento correctivo, si el sistema funciona adecuadamente, el sistema puede volver a brindar servicio, de lo contrario, se tienen que realizar las revisiones correspondientes.

Es importante que el mantenimiento correctivo se realice lo más rápido posible, ya que al ser una situación inesperada el sistema puede permanecer sin funcionar una cantidad de tiempo considerable, por esta razón es indispensable que se cuente con un plan preventivo para evitar que sea necesario poner en marcha el plan correctivo.

(Sicma21, 2021)

4.2.3. Planes de contingencia

Los planes de contingencia son procedimientos y técnicas que se diseñan estratégicamente para ayudar a controlar una situación de emergencia y en la medida de lo posible anticiparse a los problemas que puedan surgir dentro de una organización y que llegaran a dañar su correcto funcionamiento. El propósito de los planes de contingencia es establecer medidas que ayuden a mitigar los riesgos que surjan al momento de una eventualidad para que todo vuelva a funcionar con normalidad dentro de la organización en el menor tiempo posible.

Un plan de contingencia sirve para superar los impactos a los que pudiera estar expuesta la organización, esto se logra especificando acciones concretas que sean de utilidad para cada una de las situaciones que se presenten, esto quiere decir, que un plan de contingencia ayuda a mejorar la seguridad y adicionalmente sirve para optimizar recursos materiales y humanos en caso de ser necesario, con esto se puede notar que los planes de contingencia son indispensables para complementar la seguridad.

Los planes de contingencia se pueden elaborar en los diferentes niveles de la organización, es decir, puede haber planes que solucionen problemas en un equipo de trabajo, hasta planes que ayuden a mitigar riesgos potenciales dentro de una organización.

Para elaborar un plan de contingencia eficiente debe de seguirse una serie de pasos, los cuales se listan a continuación:

1. **Realizar una lista de los riesgos:** antes de comenzar a elaborar un plan de contingencia deben de tenerse identificados los riesgos que puedan surgir.
2. **Evaluar los riesgos de acuerdo a su gravedad y probabilidad de ocurrencia:** es decir, hay que hacer una evaluación de los riesgos identificados en función de dos métricas, la primera de ellas es la gravedad del impacto en la organización, y la segunda es la probabilidad de ocurrencia del riesgo.
   Los diferentes riesgos que podrían presentarse pueden observarse en la figura 4.3:

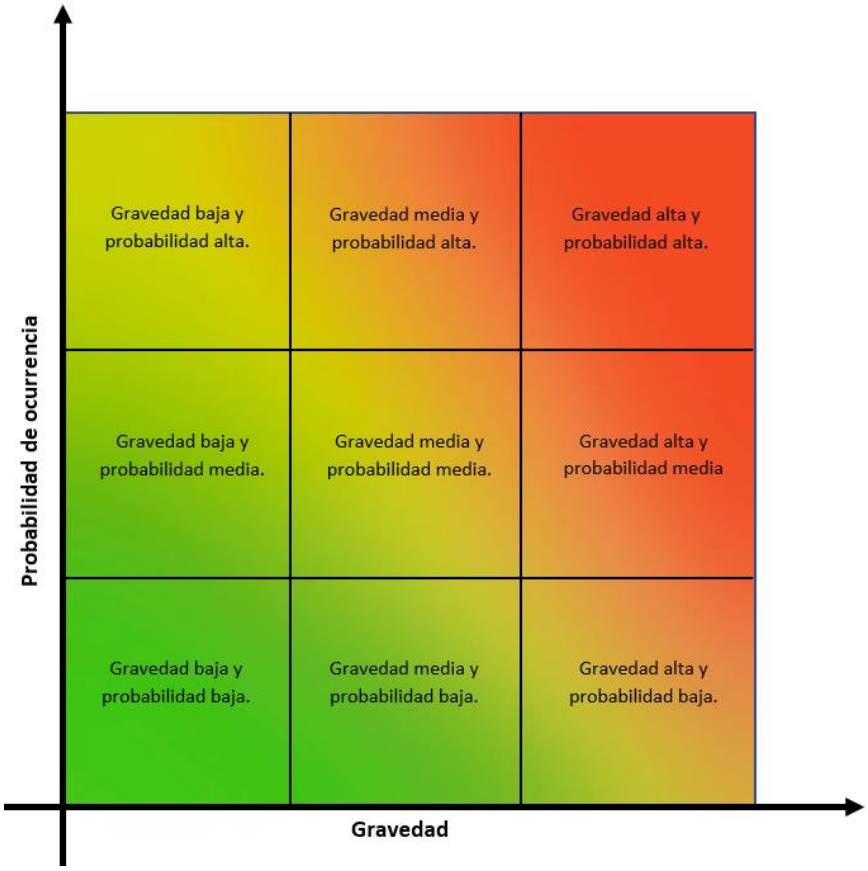


Figura 4.3. Evaluación de riesgos por probabilidad e impacto.

En la figura anterior, con la representación usando colores, se puede visualizar de una mejor manera la gravedad y probabilidad de ocurrencia de los riesgos, siendo que las probabilidades de ocurrencia bajas junto con los niveles de gravedad bajos representan un menor problema comparado con las gravedades y probabilidades de ocurrencia altas.

3. **Identificar los riesgos más importantes:** después de haber clasificado los riesgos en función de su gravedad y probabilidad de ocurrencia hay que dividirlos desde los que tienen una gravedad y probabilidad de ocurrencia alta hasta los que tienen una gravedad y probabilidad de ocurrencia más baja, esto con la finalidad de empezar a elaborar los planes de contingencia por aquellos riesgos que representen un mayor problema.
4. **Crear un plan de contingencia para los diferentes riesgos:** este plan de contingencia deberá describir los pasos a seguir en dado caso de que uno de los riesgos ocurra.
   Las etapas de un plan de contingencia son:
   a. Evaluación.
   b. Planificación.
   c. Pruebas de viabilidad.
   d. Ejecución.
   e. Recuperación

Las etapas de evaluación, planificación y pruebas de viabilidad se refieren a la parte preventiva, la etapa de ejecución hace referencia a las acciones que se deben llevar a cabo mientras ocurre la amenaza y la etapa de recuperación define las acciones que deben realizarse para recuperarse después de que ocurrió el evento desafortunado.

5. **Obtener aprobación del plan de contingencia:** es decir, que los líderes o altos mandos conozcan el plan de contingencia y estén de acuerdo con él.
6. **Compartir el plan de contingencia:** debe compartirse con el grupo de personas de interés, esto con la finalidad de que cuando sea necesario usarlo se haga rápidamente y de manera fluida.
7. **Monitorear el plan de contingencia:** hay que monitorear el plan de contingencia frecuentemente para validar que sea correcto y siga cubriendo las necesidades iniciales, en dado caso de que las necesidades hayan cambiado, se tiene que actualizar el plan de contingencia o crear nuevos planes que cubran los nuevos riesgos.

Es importante tener presente que toda organización debe contar con planes de contingencia para atender cualquier situación emergente que pudiera llegar a presentarse. Asimismo, es necesario que los planes de contingencia sean revisados, actualizados y probados periódicamente a fin de que cuando sea necesario ponerlos en marcha operen correctamente y no se presenten situaciones adversas.

(A. González, 2018; Martins, 2022; Ortíz Anderson, s. f.; Rodríguez, 2020)

Tema 5. Análisis y gestión de los riesgos

5.1. Terminología básica

5.1.1. Activos

Los activos de una organización de acuerdo con la norma ISO 27001 son los bienes o recursos con los que cuenta una organización y que, por lo tanto, deben proteger. Dentro de estos bienes y recursos se encuentran el hardware, el software y las instalaciones, solo por mencionar algunos, y no solo las organizaciones poseen activos, ya que todas las personas tienen activos personales, dentro de los cuales se encuentran sus pertenencias, tales como una casa, un automóvil, y cualquier otro objeto de valor con el que se cuente y del cual se pueda obtener algún tipo beneficio.

Estos activos se clasifican de acuerdo a su liquidez, se pueden dividir en:

- **Activos corrientes:** son los activos que se pueden convertir en dinero en efectivo de una manera rápida. Una organización puede considerar un activo corriente a todo aquello que se convierta en dinero en efectivo en menos de un año, mientras que una persona puede considerar como activo corriente a todo aquello que se pueda convertir en dinero en efectivo en un plazo menor a 6 meses.
- **Activos no corrientes:** este tipo de activos son usados para la producción dentro de la organización por lo que su vida útil suele ser superior a un año. Ejemplos de activos no corrientes dentro de una organización son: los bienes inmuebles o los dispositivos de hardware que conforman el sistema de red de la organización.

Los activos también pueden clasificarse en activos tangibles e intangibles:

- **Activos tangibles:** como su nombre lo indica, son los activos que se pueden tocar o, dicho de otra manera, son aquellos objetos materiales que tienen valor para la organización, como el hardware o un edificio.
- **Activos intangibles:** son los bienes no materiales con los que se cuenta pero que dan valor a una organización, como las patentes, licencias o la información.

Es imprescindible mencionar que la información es uno de los activos más importantes con los que cuentan las empresas, por lo tanto, esta debe ser correctamente protegida, y como se ha visto anteriormente, la información es el principal objetivo de ataque, de esto surge que la información se tenga clasificada de acuerdo a los siguientes niveles:

- **Información confidencial:** es información de alta relevancia a la que solo pueden tener acceso las personas que cuenten con la autorización correspondiente.
- **Información de uso interno:** es aquella información a la que pueden acceder todos los miembros de la organización, inclusive a la información de cada uno de los departamentos o áreas que la conforman.
- **Información pública:** es la información que es accesible para cualquier persona.

La norma encargada de proteger los activos de información de los posibles riesgos y amenazas es la norma ISO 27001 (tema 1.2).

(Billin, s. f.; Copro, s. f.; Universidad Oberta de Catalunya, s. f.)

5.1.2. Riesgo

En la seguridad informática, un riesgo es cualquier amenaza que explote las vulnerabilidades de los activos, ocasionando pérdidas. Una organización es propensa a riesgos cuando tiene vulnerabilidades que afecten a la triada CID.

En la seguridad informática siempre se ha buscado que los riesgos sean prevenidos o evitados, y en primera instancia, se podría pensar que con la tecnología que existe en la actualidad es fácil crear sistemas cuya triada CID esté completamente protegida, sin embargo, esto no es así, ya que deben de seguirse algunos requerimientos para que un sistema sea funcional, y estos requerimientos tienen conflictos entre sí, por lo que es prácticamente imposible crear un sistema completamente libre de vulnerabilidades, es decir, se puede minimizar la ocurrencia de riesgos, pero no se pueden evitar.

El objetivo principal de la gestión de los riesgos es minimizar su ocurrencia, además le permite a una organización conocer su nivel de seguridad, lo cual hará que la organización realice un análisis donde pueda decidir qué acciones debe tomar para minimizar la ocurrencia de los riesgos.

(G. Fernández, 2018)

5.1.3. Aceptación

La aceptación de los riesgos es una parte fundamental, ya que hace referencia a que la organización está consciente de los riesgos que se pueden presentar y, por lo tanto, pueden hacer un análisis para decidir qué medidas de seguridad deben implementar para mitigarlos, por otro lado, hay riesgos que no llegan a comprometer a la organización, por lo que pueden decidir solamente controlarlos y monitorearlos para ver su evolución.

Para aceptar un riesgo pueden tomarse como base los siguientes criterios que se muestran en la figura 5.1:

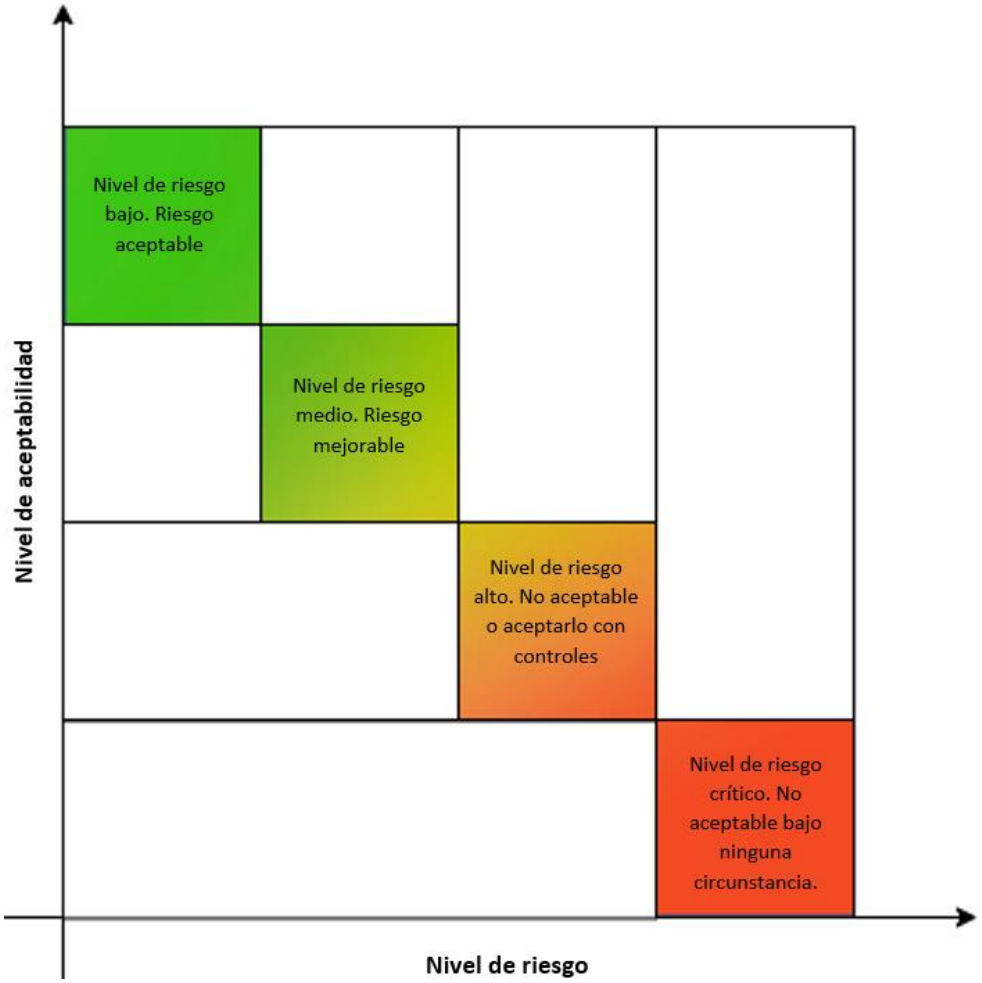


Figura 5.1. Aceptación de riesgos

Como se puede observar, cuando se tiene un nivel de riesgo bajo, el riesgo es aceptable, si se tiene un nivel de riesgo medio, el riesgo es mejorable, mientras que, si el riesgo es alto, lo ideal es no aceptarlo, sin embargo, puede aceptarse tomando medidas de seguridad. Finalmente, en caso de que el nivel de riesgo sea crítico, la organización no deberá aceptarlo bajo ninguna circunstancia.

Es importante mencionar, que cada organización debe establecer sus propios criterios de aceptación, ya que estos van a depender de las políticas que se tengan establecidas.

(Romero Pérez et al., 2021)

5.1.4. Análisis del riesgo

Un análisis de riesgos es un estudio que realiza la organización para evaluar los riesgos y sus consecuencias, con este análisis se podrán determinar los factores de riesgo que podrían causar más problemas y con ello, posteriormente establecer medidas de prevención y control.

El análisis de riesgos responde las siguientes preguntas:

- ¿Qué se quiere proteger?
- ¿Contra qué o de qué se quiere proteger?
- ¿Cómo se quiere proteger?

Realizar un análisis de riesgos ofrece las siguientes ventajas:

- Identificar cuales son los activos que tiene la organización, además de identificar las amenazas y vulnerabilidades que pueden producir los riesgos.
- Conocer los riesgos a los que está expuesta la organización con esto podrá priorizarlos para atender primero aquellos que tienen mayor probabilidad de producirse.
- Saber el impacto que tendría cada uno de los riesgos si llegaran a producirse.
- Facilitar la aplicación de medidas preventivas y correctivas, reduciendo el tiempo entre que ocurre el incidente y el tiempo en el que se atiende, para así reducir el impacto negativo causado.

El análisis de riesgos se conforma de las siguientes etapas:

1. Identificación y evaluación de los activos.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Determinación del impacto de la ocurrencia de una amenaza.
5. Determinación de controles.
6. Identificación de riesgos residuales.
7. Identificación de los controles adicionales.
8. Preparación de un informe de análisis del riesgo.

Las etapas del análisis de riesgos se explican a detalle en el tema 5.4.

Si no se hace un análisis de riesgos, la organización podría carecer de medidas de seguridad importantes, por lo que se vería afectada de diferentes maneras como con pérdida de actividad o pérdida de datos sensibles.

(Grupo ACMS Consultores, s. f.; Pirani, s. f.-b; UNAM, s. f.-c)

5.1.5. Manejo del riesgo

El manejo del riesgo es un proceso que consiste en identificar y controlar los riesgos para minimizarlos, al hacer esto, las organizaciones pueden enfrentarlos a costos más bajos, teniendo pérdidas menores si algún riesgo llegara a presentarse.

5.1.6. Evaluación

En la evaluación de riesgos se hace un análisis de las consecuencias que tiene un activo al estar expuesto a las posibles amenazas que exploten sus vulnerabilidades. En esta evaluación se identifica la gravedad del riesgo detectado para determinar la prioridad con la que será atendido.

Para realizar la evaluación de riesgos se puede usar alguno de los siguientes métodos:

- **Método cualitativo:** este tipo de análisis se realiza sobre datos no numéricos, es útil cuando no es posible realizar un análisis estadístico o es necesario evaluar las características de los activos.
- **Método cuantitativo:** usa herramientas matemáticas para calcular la probabilidad de ocurrencia de un riesgo, esto significa que este método cuantifica los riesgos de acuerdo a su probabilidad de ocurrencia e impacto.

El método cuantitativo y cualitativo serán explicados con más detalle en los temas 5.2 y 5.3 respectivamente.

(Pirani, s. f.-b)

5.1.7. Impacto

El impacto hace referencia a las pérdidas o consecuencias que se ocasionan después de que una vulnerabilidad de un activo fue explotada. Generalmente, el impacto se estima en porcentaje, donde el 100% es la pérdida total del activo.

Para medir el impacto se hace mediante una escala, la cual es definida por la organización. Un ejemplo de escala es el siguiente:

Tabla 5.1. Impacto.

Impacto	Posibles consecuencias
Nulo	El riesgo en la organización no provoca problemas.
Mínimo	El riesgo provoca problemas menores en la organización.
Medio	El riesgo puede causar pérdidas momentáneas.

Alto	El riesgo puede causar que la organización tenga pérdidas considerables.
Muy alto	El riesgo puede causar que la organización detenga sus actividades por completo.

Dependiendo del impacto que tenga el riesgo en la organización, es como se decide en qué prioridad van a ser atendidos cada uno de los riesgos.

(M. M. Jiménez, 2021; Romero Pérez et al., 2021)

5.1.8. Pérdida esperada

La pérdida esperada puede definirse como el nivel de impacto que espera tener una organización después de que la vulnerabilidad de un activo haya sido explotada.

5.1.9. Vulnerabilidad

Debilidad en un sistema que puede explotarse, con la finalidad de perjudicarlo, afectando a la triada CID, por lo que es de suma importancia detectar las vulnerabilidades presentes para eliminarlas. Las vulnerabilidades pueden tener origen en el diseño del sistema o errores de configuración, solo por mencionar algunos.

En el tema 2.2 se explica más a detalle este tema, donde también se incluyen los tipos de vulnerabilidades.

5.1.10. Amenaza

Posibilidad de que ocurra un evento que ponga en riesgo la seguridad de un sistema, provocando daños y/o pérdidas a una organización, en otras palabras, las amenazas son acciones que se aprovechan de las vulnerabilidades para provocar daños.

En el tema 2.1 ya se explicó más a detalle este tema, incluyendo las fuentes de amenaza.

5.1.11. Riesgo residual

Los riesgos residuales, de acuerdo con la ISO 27001, son aquellos que permanecen después de haber tomado las acciones correspondientes para controlarlos, ya que, como se mencionó, es imposible eliminar los riesgos por completo, sin embargo, es importante saber el nivel de los

riesgos residuales, ya que previamente se les aplicaron medidas de mitigación, por lo que deberían de monitorearse hasta que el riesgo tenga un nivel aceptable.

(Escuela Europea de Excelencia, 2019; Reyes Castro & Porras Garzón, s. f.)

5.1.12. Controles

Los controles son un conjunto de mecanismos los cuales le permiten a las organizaciones cumplir sus políticas de seguridad. Estos controles tienen como objetivo analizar qué tan efectivas son las medidas de protección que la organización implementó, para que en caso de ser necesario puedan mejorarlas.

(GlobalSuite Solutions, 2021; Romero Pérez et al., 2021)

5.2. Análisis cuantitativo

El análisis cuantitativo de riesgos hace uso de técnicas y herramientas de matemáticas y estadística, con las cuales se puede hacer un cálculo aproximado de que tan probable es que ocurra un riesgo, este cálculo puede hacerse con muestras numéricas, por lo que si los resultados son extrapolados se puede obtener más información, también, es posible realizarlo con datos recopilados anteriormente de los riesgos e impactos que ha tenido la organización.

Posteriormente, con los datos recogidos la organización puede predecir o estimar los resultados para tener un panorama más amplio del impacto de los riesgos. De manera general, el valor que se asocia a los riesgos en un análisis cuantitativo se da en porcentaje.

Este tipo de análisis está basado en la probabilidad de ocurrencia de un riesgo y en las pérdidas que habría si es que el riesgo se llega a producir, o, dicho de otra manera, el análisis cuantitativo cuantifica los riesgos de acuerdo a su probabilidad de ocurrencia e impacto.

Las pérdidas pueden calcularse con la fórmula ALE (Annualized Loss Expectancy o Expectativa de Pérdida Anual), ésta es una fórmula algebraica con la que se puede modelar el impacto de los riesgos de seguridad sobre los activos, dicha fórmula también muestra una relación costo – beneficio, con la cual la organización podrá asignar los recursos necesarios para disminuir la cantidad de pérdidas si un riesgo se llegara a producir.

La definición de la fórmula es la siguiente:

$$ALE = SLE * ARO$$

Donde:

- **ALE – Expectativa de Pérdida Anual:** indica la pérdida total monetaria que puede esperar la organización si un riesgo se materializa, este valor monetario se indica usando la moneda local donde la organización está ubicada.
- **SLE – Expectativa de pérdida individual:** indica la pérdida monetaria que espera tener la organización si un activo se ve comprometido, este valor se indica usando la moneda local donde está ubicada la organización.
- **ARO – Tasa de ocurrencia anualizada:** es un valor expresado en porcentaje que indica la probabilidad de que un riesgo se vea comprometido en un periodo de un año.

Lo anterior significa que con la fórmula ALE se calcula la pérdida total esperada para un activo cuando una o más amenazas se materializan en un periodo de un año.

Mientras tanto, la SLE se calcula como:

$$SLE = FE * VA$$

Donde:

- **FE – Factor de exposición:** es un valor en porcentaje que indica la cantidad de valor que pierde el activo cuando un determinado riesgo se materializa.
- **VA – Valor del activo:** indica el valor que tiene el activo para la organización. Este valor se indica usando la moneda local del lugar donde se encuentra la organización.

Es decir, el SLE se calcula como el factor de exposición del activo, multiplicado por el valor del activo en cuestión.

Para ejemplificar lo anterior, se supondrá que una organización cuenta con un servidor del cual se quiere obtener su ALE y SLE.

Hay que tomar en cuenta que el valor del activo en cuestión es el valor que tiene dicho activo para la organización, sumado al costo monetario del activo, por lo que para calcular este valor debe considerarse entre otras cosas la cantidad y el tipo de información que almacena.

Los datos que se tienen para hacer los cálculos correspondientes son los siguientes:

Tabla 5.2. Cálculo de ALE.

Activo	Amenaza	VA	FE	ARO
Servidor	Factor humano intencional	$2,000,000	25%	30%

Antes de obtener el ALE, debe calcularse el SLE:

- *SLE = FE * VA*
- *SLE = 0.25 * $2,000,000*
- *SLE = $500,000.*

Una vez calculado el valor de SLE se puede calcular el ALE:

- *ALE = SLE * ARO*
- *ALE = $500,000 * 0.3*
- *ALE = $150,000*

Por lo tanto, la expectativa de pérdida anual esperada para el servidor es de $150,000, suponiendo que en un año únicamente fue afectado por el factor humano de manera intencional. Para obtener resultados más precisos, deben considerarse todas las amenazas a las que se expone el activo y para obtener el ALE total debe realizarse la sumatoria de todos los ALE intermedios.

La organización debe tener en cuenta que si el valor del ALE es mayor al costo del activo es necesario aplicar medidas de seguridad, sin embargo, se debe considerar que el costo por

implementar los controles necesarios debe ser menor al valor del activo, esto se explica de una mejor manera en el tema 5.5.

El análisis cuantitativo beneficia a todo tipo de organizaciones, ya que independientemente del sector, ayudará a identificar los riesgos, consecuencias e incluso una frecuencia estimada de ocurrencia, con el objetivo de mantener los niveles de riesgo dentro de valores aceptables.

Este tipo de análisis es más complicado de realizarse comparado con el análisis cualitativo, esto se debe a que en el análisis cuantitativo se deben considerar muchos factores para obtener resultados precisos, sin embargo, si se realizan ambos análisis se obtienen resultados más completos.

(Cruzito, 2020; Mendoza, 2014a, 2015)

5.3. Análisis cualitativo

El análisis cualitativo se realiza sobre datos que no son cuantificables, por lo que se valoran las características de los activos. El objetivo de este tipo de análisis es asignar un nivel de prioridad a los riesgos para que los responsables de la gestión de riesgos tomen decisiones que les permitan definir una estrategia para mitigar o controlar cada uno de los riesgos identificados.

Este análisis al realizarse sobre datos no cuantificables, los resultados que se obtienen no son cuantificables, es decir, a los riesgos se les asigna una clasificación, basada en la percepción de la probabilidad de ocurrencia y del impacto, esto va a depender de las necesidades de la organización o del tipo de riesgo, esta clasificación puede ser baja, media, alta o similares. Es posible que algunos riesgos se materialicen en más de una ocasión, en este caso también debería evaluarse la frecuencia con la que ocurren.

Al ser clasificados de esta manera, se dice que el análisis cualitativo es un análisis subjetivo, de esto surge la necesidad de que los criterios que se hayan definido para hacer dicha clasificación deben ser muy precisos para evitar confusiones. Una ventaja de clasificar los riesgos de esta manera es que es más fácil comprender que los riesgos con clasificaciones altas tienen mayor prioridad sobre los riesgos que tienen clasificaciones más bajas.

Cabe mencionar que para que el análisis cualitativo sea exitoso, debe contarse con datos de calidad, es por ello que durante un proyecto o el ciclo de vida del sistema este tipo de análisis debería realizarse de manera periódica, ya que pueden surgir nuevos riesgos o los existentes podrían evolucionar.

Para realizar el análisis cualitativo puede usarse alguna de las siguientes técnicas:

- **Lluvia de ideas:** consiste en realizar reuniones, en las cuales los interesados deben compartir sus puntos de vista acerca de los riesgos que hay o de los nuevos que pueden surgir. Ésta es una técnica muy interesante, ya que cada quien tendrá puntos de vista diferentes, por lo que podrán complementarse entre sí para obtener mejores resultados.
- **Entrevistas:** estas pueden ser semiestructuradas o abiertas, esto dependerá del riesgo y de la información que se quiere obtener. Las entrevistas pueden ser una técnica bastante útil, debido a que ayudarán a recopilar información de las posibles situaciones de riesgo, así como del comportamiento del activo cuando se encuentra en riesgo.
- **Cuaderno de registros:** en esta técnica se toman notas de las posibles causas y consecuencias de las situaciones de riesgo, para priorizar las situaciones que representen un mayor peligro para la organización.

Lo ideal es que para realizar un buen análisis cualitativo se use una combinación de las técnicas adecuadas para el tipo de información que se quiere obtener, hay que recordar que para que este método sea eficiente se debe tener información precisa.

De manera general, hay cuatro pasos a seguir para realizar el análisis de riesgos cualitativo:

Paso 1. Identificar los riesgos.

Se debe crear una lista en donde se muestren los riesgos a los que se exponen los activos.

Paso 2. Clasificar los riesgos.

Para este paso, hay diferentes técnicas de clasificación, sin embargo, la técnica más usada es la matriz de riesgos, donde se clasifican los riesgos de acuerdo con su probabilidad de ocurrencia y el impacto que causarían si llegaran a materializarse, un ejemplo de una matriz de riesgos es la que se observa en la figura 5.2.

Impacto / Probabilidad	Muy bajo	Bajo	Medio	Alto	Crítico
Altamente probable	Importante	Alto	Muy alto	Intolerable	Inaceptable
Muy probable	Moderado	Importante	Alto	Muy alto	Intolerable
Medianamente probable	Tolerable	Moderado	Importante	Alto	Muy alto
Poco probable	Bajo	Tolerable	Moderado	Importante	Muy alto
Muy poco probable	Trivial	Bajo	Tolerable	Moderado	Muy importante

Figura 5.2. Matriz de riesgos.

La figura anterior, muestra la clasificación de los riesgos acorde a la probabilidad de ocurrencia e impacto, en dicho ejemplo, se tienen diferentes niveles de clasificación, los cuales van desde trivial hasta inaceptable, estas clasificaciones, así como los niveles de probabilidad e impacto cambian dependiendo del tipo de riesgo que se esté tratando, por lo que la organización es libre de adecuarlo a sus necesidades, así como de elegir los criterios para hacer su clasificación de riesgos.

Paso 3. Controlar los riesgos.

Consiste en definir las técnicas de mitigación para minimizar la probabilidad de la ocurrencia de riesgos y su impacto, es decir, se analizan las causas de los riesgos, dentro de las cuales pueden estar los procesos de gestión poco eficaces que se tienen implementados, asimismo, mediante la implementación de acciones correctivas se puede reducir el impacto negativo de los diferentes riesgos.

Paso 4. Controlar los riesgos empresariales.

Es importante hacer un seguimiento de los riesgos, para esto, deben guardarse las observaciones realizadas durante todo el proceso del análisis cualitativo. En este paso, lo principal es observar los riesgos para responder las siguientes preguntas:

- ¿Es eficaz el control de riesgos?
- ¿Se han clasificado correctamente los riesgos?
- ¿Se han identificado todos los riesgos?

En el análisis de riesgos, ambos tipos de análisis son importantes, ya que no siempre se podrá realizar un análisis cuantitativo porque no todas las situaciones lo van a permitir. Ambos tipos de análisis se complementan, por lo que, de ser posible, lo ideal sería analizar las situaciones de riesgo usando ambos métodos para obtener mejores resultados al momento de implementar medidas de seguridad.

(Alcántara, 2019; Guerrero, 2020; Mendoza, 2015)

5.4. Etapas del análisis del riesgo

5.4.1. Identificación y evaluación de los activos

Como se mencionó en el tema 5.1, los activos son los bienes y recursos con los que cuenta una organización los cuales debe proteger, ya que estos pueden o no depender de otros activos que en conjunto ayudan a la organización a cumplir sus objetivos.

Inicialmente, se deben definir todos los activos que se quieren proteger, estos pueden ser tangibles o intangibles, como los que me mencionan a continuación:

- **Información:** son todos los datos que la organización genera y/o procesa. La información es considerada el activo más importante de cualquier organización, por lo que es necesario tomar en cuenta la información almacenada en medios físicos y electrónicos.
- **Software:** hace referencia a las aplicaciones y programas que son usados por los empleados de la organización para manejar información.
- **Hardware:** se refiere a los dispositivos físicos que conforman el sistema, los cuales almacenan, procesan o transportan información.
- **Usuarios:** es importante tomarlos en cuenta porque son quienes interactúan directamente con los sistemas y la información, pueden dividirse en:
    - **Usuarios internos:** son los usuarios que conforman la empresa, tienen niveles jerárquicos y dependiendo de su nivel es su participación en la toma de decisiones internas de la organización. Entre algunos de los usuarios internos se encuentran:

        - Propietarios, accionistas, gerentes, administradores y trabajadores.
    - **Usuarios externos:** son aquellos que requieren conocer información de la organización para tomar algunas decisiones, sin embargo, este tipo de usuarios no pertenece directamente a la organización. Entre este tipo de usuarios se encuentran: proveedores, auditores, clientes y público en general.
- **Instalaciones:** es importante su protección ya que en las instalaciones es donde se encuentran los demás activos de la organización.

Para saber cuál es la importancia de los activos, se debe comprender cual es la misión de la organización, comprendiendo esto, será posible hacer una distinción entre los activos que hacen que la organización funcione adecuadamente y aquellos activos que dependen de otros para funcionar.

Lo anterior es de suma importancia, porque la organización al tener claros cuales son los activos que dependen de otros y cuales son independientes podrá tomar las acciones necesarias para mantener un funcionamiento continuo en caso de haya problemas con alguno de los activos.

(Toro, 2017; UNAM, s. f.-c)

5.4.2. Identificación de amenazas

Después de que se tienen identificados los activos que la organización quiere proteger deben de identificarse las amenazas a las que cada uno de esos activos está expuesto, es importante recordar que una amenaza se define como la posibilidad de ocurrencia de un evento accidental o intencionado que ponga en riesgo la seguridad, pueden provocar desde daños pequeños y fáciles de controlar, hasta pérdidas financieras o de información, como se mencionó en el tema 2, las amenazas se clasifican en cinco tipos:

- Desastres naturales.
- Errores de hardware.
- Errores en la red.
- Humanas.
- Lógicas.

Después de que se identificó la fuente de amenaza a la que cada uno de los activos está expuesto, se debe analizar el entorno de los activos, esto con la finalidad de hacer un análisis para concluir la probabilidad de que dicha amenaza ocurra teniendo en cuenta las condiciones en las que se encuentran los activos a proteger.

Teniendo en cuenta lo anterior, se puede asignar una clasificación a cada una de las amenazas identificadas:

- **Baja:** la amenaza nunca ha ocurrido y es muy poco probable que ocurra.
- **Media:** la amenaza ha ocurrido en ocasiones anteriores, y ha sido controlada antes de ocasionar daños graves.
- **Alta:** es muy probable que la amenaza ocurra y traiga consigo graves daños a la organización.

En esta etapa, al realizar la identificación de amenazas, es importante también identificar a los distintos tipos de atacantes que estén interesados en violar la seguridad de la organización, ya sea para tener acceso a información confidencial o para causar daños más graves, como alterar la información u ocasionar un ataque que afecte la infraestructura del sistema, de igual manera hay que tener presente que es necesario tomar en cuenta que usuarios del mismo sistema pueden causar daños a la organización de manera accidental.

Finalmente, después de haber analizado las amenazas y los tipos de atacantes, hay que hacer un análisis donde se identifiquen las consecuencias que tendría la organización si la amenaza se llevara a cabo, ya que, las consecuencias son diversas y tienen diferentes niveles de gravedad, dichas consecuencias pueden ir desde la caída del sistema por unos minutos, hasta el robo y/o alteración de información confidencial.

(UNAM, s. f.-c)

5.4.3. Identificación de vulnerabilidades

Posterior a la identificación de amenazas se tienen que identificar las vulnerabilidades. Como se mencionó en el tema 2, una vulnerabilidad es una debilidad que al explotarse puede causar daños o pérdidas, por lo que es importante identificarlas.

En un análisis de vulnerabilidades además de evaluar los riesgos y amenazas, se tienen que definir e identificar las vulnerabilidades que puedan estar presentes en los activos que se quieren proteger, para después priorizar las debilidades encontradas y atenderlas de acuerdo a su nivel de importancia.

Los análisis de vulnerabilidades son muy útiles para hacer una evaluación de riesgos y así buscar soluciones que ayuden a aumentar la seguridad y al mismo tiempo reducir la probabilidad de éxito de los ataques.

En los análisis de vulnerabilidades, se tiene un ambiente controlado, en donde se usan herramientas para realizar pruebas de intrusión, y mediante diferentes actividades se detectan y explotan las debilidades encontradas que ponen en riesgo a la organización.

Dentro de los objetivos del análisis de vulnerabilidades se encuentran:

- Identificar que vulnerabilidades de los activos pueden poner en riesgo la seguridad de la organización.
- Ayudar a decidir cuándo se deben sustituir piezas de hardware o software antes de que provoquen daños o pérdidas.
- Optimizar las configuraciones de software con el objetivo de reducir la ocurrencia de ataques.
- Apoyar en la mejora continua de los controles de seguridad implementados.
- Documentar el nivel de seguridad de la organización, esto puede usarse para demostrar el cumplimiento de políticas, reglamentos y leyes.

Al término del análisis de vulnerabilidades se tiene que generar un informe, éste deberá contener las vulnerabilidades que se encontraron y una clasificación del riesgo que representan, esta parte es muy importante, porque con este informe la organización podrá definir acciones para corregir dichas vulnerabilidades y a su vez, tomar las medidas necesarias para minimizar la ocurrencia de ataques.

(SayNet, s. f.)

5.4.4. Impacto de la ocurrencia de una amenaza

Cuando una amenaza es explotada, la organización sufre diversos daños, esto es mejor conocido como impacto. El impacto indica cuales son las consecuencias que tendrá que enfrentar una organización cuando una amenaza se materializa.

Muchas veces, cuando una amenaza es explotada, no solo se ve afectado un activo, hay veces que la reacción es en cadena, por lo que se ven afectados un grupo de activos, es por ello que el impacto se valora tomando en cuenta los daños que produjo la amenaza explotada a la organización, asi como los daños producidos en el propio activo. Generalmente, el impacto se estima en porcentaje, donde el 100% significa que el activo en cuestión se ha perdido por completo.

Entre los impactos que se pueden generar por la materialización de una amenaza se encuentran:

- Pérdidas económicas.
- Pérdida de productividad.
- Pérdida de clientes.
- Pérdida de credibilidad, imagen y reputación.
- Pérdida de diferenciación dentro del mercado.
- Pérdida en la continuidad del servicio que se ofrece.

Las diferentes pérdidas que sufre una organización se clasifican dentro de las siguientes áreas de impacto:

- **Revelación:** hace referencia a que se pierde la confidencialidad de la información.
- **Modificación:** se refiere a que el atacante modifica la información de la organización, es decir se ve afectada la integridad de la misma.
- **Denegación:** hace referencia a cuando la organización pierde de manera temporal disponibilidad de los servicios que ofrece.
- **Destrucción:** se refiere a cuando el activo se pierde por completo.

Es muy importante que las organizaciones estén conscientes de los diferentes impactos que pueden sufrir cuando se produzca una amenaza, esto con la finalidad de que actúen de forma inmediata para disminuir dicho impacto.

(Jiménez, 2021)

5.4.5. Controles en el lugar

Son medidas de seguridad que toma la organización para gestionar los riesgos encontrados duramte el análisis de riesgos, éstas ayudan a prevenir o mitigar los riesgos a los que se expone una empresa u organización, aumentando así, la probabilidad de éxito de los objetivos establecidos.

Después de haber identificado todos los riesgos, se deben de tomar las medidas de seguridad necesarias para enfrentar dichos riesgos. De análisis anteriores, es posible que la organización ya tenga algunos controles establecidos, si este es el caso, estos controles deben de revisarse para verificar que sean los adecuados y que cubran las necesidades de la organización, de no ser así, deben ser actualizados o en caso de ser necesario deben eliminarse por completo y crear nuevos controles de seguridad que cubran de una manera eficiente las necesidades de la organización para que ésta alcance sus objetivos.

Después de crear los controles, se debe verificar su efectividad para comprobar si funcionan adecuadamente para lo que fueron diseñados, asimismo, se debe de verificar que los responsables de ejecutar los controles conozcan los mismos a la perfección, esto con la finalidad de aplicarlos correctamente y así obtener mejores resultados, también, es posible que los responsables necesiten ser capacitados para que puedan aplicar los controles adecuadamente.

Es posible que la organización tenga muchos controles diseñados para enfrentar los diferentes riesgos, y quizá se tenga la creencia de que entre más controles estén implementados es mejor, sin embargo, esto no es así, solo deben conservarse los controles que cubran de mejor manera

las necesidades de la organización y eliminar aquellos que las cubran parcialmente para evitar confusiones en el momento de su aplicación.

(Reyes Castro & Porras Garzón, s. f.; UNAM, s. f.-c)

5.4.6. Riesgos residuales

Los riesgos residuales de acuerdo con la norma ISO 27001, se definen como aquellos que permanecen después de implementar los controles necesarios para mitigar los riesgos que se identificaron en el análisis de riesgos.

La identificación de riesgos residuales se realiza igual que como que identifican los riesgos, es decir, se usan las mismas herramientas, metodologías y escalas de evaluación

Cabe mencionar que la mayoría de los riesgos no van a poder eliminarse por completo, por lo que después de haber aplicado los controles de seguridad necesarios para reducir su impacto hay que verificar si el nivel de riesgo residual está dentro de los niveles de riesgo aceptables considerados por la organización.

Después de hacer el análisis de riesgos residuales e identificarlos, se tienen dos opciones:

1. **El nivel de riesgo residual se encuentra por debajo de los niveles aceptables:** cuando es así, ya no es necesario implementar nuevas medidas, ya que, al estar debajo de los niveles aceptables, la organización acepta el nivel de riesgo y convive con él.
2. **El nivel de riesgo supera los límites tolerables:** en este caso, se deben implementar controles de seguridad más eficaces, los cuales brinden más seguridad a la organización.

Los riesgos residuales van a proporcionar información acerca de las oportunidades de mejora ya que muestran qué tan vulnerable queda la organización después de enfrentarse a algún tipo de riesgo, asimismo, proporcionan información acerca de la capacidad de recuperación de la organización.

(Escuela Europea de Excelencia, 2019; Reyes Castro & Porras Garzón, s. f.; UNAM, s. f.-c)

5.4.7. Identificación de los controles adicionales

Después de haber identificado los riesgos residuales se debe identificar el nivel de cada uno de esos riesgos para determinar si están en un nivel aceptable para la organización o no. La organización es la que va a determinar si los riesgos residuales se encuentran en un nivel aceptable, el que lo estén o no va a depender de las políticas de seguridad que se tienen implementadas, así como del entorno de la organización, por lo que la alta dirección es la responsable de determinar cuáles son esos niveles aceptables.

En dado caso, de que se determine que los riesgos residuales no se encuentran dentro de los niveles aceptables, es cuando se deben de identificar controles de seguridad adicionales, mediante los cuales la organización llevará cada uno de los riesgos a un nivel aceptable.

(Reyes Castro & Porras Garzón, s. f.; UNAM, s. f.-c)

5.4.8. Preparación de un informe del análisis del riesgo

Como último paso del análisis de riesgos se deberá elaborar el informe del análisis de riesgos. Este informe permite dar a conocer la información más importante asociada a los riesgos a los cuales está expuesta la organización, así como las acciones que deben llevarse a cabo para mitigarlos.

Este informe de análisis de riesgos debe contener lo siguiente:

- **El nivel de vulnerabilidad de cada uno de los activos analizados:** es necesario identificar para cada activo su nivel de participación y vulnerabilidad.
- **Las amenazas detectadas durante el análisis:** se recomienda que al hacer este análisis se identifiquen las amenazas existentes, para posteriormente implementar las medidas de seguridad.
- **La probabilidad de ocurrencia del riesgo, asi como su nivel de prioridad:** esto es importante, para saber el nivel de prioridad con el que deben atenderse, ya que se pondrá mayor atención en aquellos riesgos que tengan una probabilidad de ocurrencia más elevada y que afecten mayormente a la organización.
- **Los controles que se van a implementar para la mitigación de los riesgos:** es de los puntos más sobresalientes en el informe de análisis de riesgos, ya que explicará las medidas que deberán implementar los encargados de seguridad para mitigar los riesgos. De igual manera deberá explicar a los demás miembros de la organización las acciones con las que deberán contribuir para mejorar la seguridad.
- **El riesgo residual al que se expone la organización:** es altamente recomendable que en la organización se sepan los niveles de riesgo que se tendrán después de haber implementado los controles de seguridad, para saber si hay que implementar controles adicionales o simplemente vigilar los riesgos para mantenerlos bajo control.
- **La pérdida esperada:** es indispensable que la organización esté consciente de las pérdidas que tendría si un riesgo llegara a materializarse.

(GraphEverywhere, 2020; UNAM, s. f.-c)

5.5. Análisis costo – beneficio

El análisis costo – beneficio es un proceso que sirve para elegir de un conjunto de opciones aquellas que darán mayores beneficios a la organización, es decir, hace una evaluación de los gastos que hará la organización, así como un estimado de los recursos que empleará para implementar la protección de los activos, adicionalmente, proporciona los beneficios económicos de cada una de las opciones para decidir con cuales es viable continuar.

Este tipo de análisis es cuantitativo, ya que ayuda a la organización a tomar decisiones basándose en evidencias y no en opiniones, evitando así, que se tenga preferencia por decisiones que no brinden los mayores beneficios a la organización.

Al momento de realizarse el análisis de riesgos deben de tenerse en cuenta los siguientes costos para posteriormente realizar el análisis costo – beneficio:

- **Ca – costo del sistema:** es decir, el valor de los activos que se van a proteger.
- **Cm – costo de los medios:** se refiere al costo que necesitaría cubrir el atacante para destruir las medidas de seguridad de la organización.
- **Cs – costo de las medidas de seguridad:** se refiere a los costos de la organización para proteger cada uno de los activos.

Para que una organización sepa si las medidas de seguridad que pretende implementar son viables debe cumplirse la siguiente relación:

$$Cm > Ca > Cs$$

La relación anterior, implica que el costo que tendría que cubrir el atacante debe ser mayor al costo del sistema que desea atacar, y a su vez el costo del sistema debe ser mayor al costo de las medidas de seguridad implementadas.

El análisis costo – beneficio puede usarse en las siguientes situaciones:

- Desarrollo de nuevas estrategias de negocios.
- Toma de decisiones para asignar recursos.
- Decidir si se avanza o no con un nuevo proyecto.
- Comparar las oportunidades de inversión.
- Evaluar los cambios en la estructura de los procesos corporativos.

Para saber si se están tomando buenas decisiones, en el análisis costo – beneficio se tiene que asignar un valor monetario a todas las decisiones que implican costos y beneficios, después, se tiene que hacer la sumatoria de todos los costos que implica proteger cierto activo o tomar una decisión, a ese resultado se le tiene que restar el total de los beneficios, con esto se determina cual es la ganancia neta, si como resultado se tiene que la cantidad de beneficios supera a la cantidad de costos se asume que se están tomando buenas decisiones, mientras

que, si la cantidad de costos supera los beneficios, es un indicador de que se están tomando malas decisiones, por lo que la organización debería tomar en cuenta alguna de las otras opciones que le aporte mejores beneficios.

(López Barrientos & Quezada Reyes, 2019; UNAM, s. f.-c)

5.5.1. Metodologías certificadas de los análisis de riesgos.

Las metodologías de análisis de riesgos son un conjunto de técnicas usadas para evaluar los riesgos que pueden presentarse en una organización, con estas metodologías las organizaciones podrán tomar decisiones certeras al implementar medidas para disminuir la ocurrencia de riesgos o reducir el impacto de algún riesgo que llegara a producirse.

El análisis de riesgos debe ayudar a identificar, evaluar y manejar los diferentes tipos de riesgos de la organización, además debe ayudar a tomar buenas decisiones para mejorar su seguridad, asimismo, debe orientar a la organización para elegir una combinación de medidas las cuales aporten un buen nivel de seguridad a la organización a un costo razonable.

Hacer un análisis de riesgos trae consigo una serie de beneficios, los cuales van a ser diferentes para cada una de las organizaciones, sin embargo, dichos beneficios se verán reflejados en el análisis costo beneficio. Entre los beneficios que una organización puede obtener al realizar un análisis de riesgos se encuentran:

- Asegurar que la organización opere de manera continua.
- Elaborar una estrategia de protección, la cual ayude a disminuir los riesgos.
- Facilitar la toma de decisiones para tener certeza económica y financiera.
- Tener planes de acción para manejar correctamente las amenazas y riesgos.
- Justificar los costos por implementación de medidas de seguridad.
- Permitir que los integrantes de la organización participen en la puesta en marcha de las medidas de seguridad, volviendo esto parte de la cultura de la organización.

Hay diferentes metodologías para realizar los análisis de riesgos, por lo que la mejor forma de realizar dicho análisis es combinando las técnicas que mejor se adecuen a las necesidades de la organización. Algunas de estas metodologías son:

5.5.1.1 OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation

La metodología Operationally Critical Threat, Asset and Vulnerability Evaluation por sus siglas en inglés OCTAVE en español conocida como Evaluación de Amenazas, Activos y

Vulnerabilidades Operativamente Criticas, fue desarrollada en el Centro de Coordinación del Instituto de Ingeniería de Software en la Universidad Carnegie Mellon de Pensilvania en Estados Unidos en 1999. Esta es una metodología de análisis y gestión de riesgos, cuyo propósito es mantener seguros a los sistemas informáticos de las organizaciones, esto lo logra evaluando los riesgos, y con los resultados que obtiene sugiere un plan para mitigarlos. OCTAVE también concientiza a los miembros que conforman la organización para que comprendan que la seguridad informática es algo en lo que todos deberían cooperar ya que no solo se ve involucrada la seguridad de la información, el hardware o las instalaciones, para esto, proporciona información sobre otros estándares los cuales es recomendable que use la organización para complementar la seguridad tanto en los aspectos técnicos, como en los no técnicos.

Esta metodología sirve de guía a la organización para que con las decisiones que tomen protejan sus activos e infraestructura, además al usar OCTAVE, las organizaciones aprenderán a identificar y evaluar sus riesgos de seguridad, así como crear los planes de mitigación necesarios, con lo cual las organizaciones cumplirán con los requisitos de seguridad de la información.

OCTAVE consta de tres fases principales, y cada una de estas fases se compone de diferentes procesos:

Fase 1. Identificación de activos.

Durante esta primera fase, se deben identificar los activos que soportan los servicios informáticos de la organización, posteriormente se evalúa cada uno de ellos para identificar los activos más importantes, es decir, aquellos que hacen que la organización funcione adecuadamente, después de realizar esto, se deben de identificar las amenazas a las cuales se exponen dichos activos.

Esta metodología divide los activos de la organización en dos tipos, el primero de ellos son los sistemas, dentro de los cuales se incluyen el hardware, el software y los datos. El segundo tipo de activo hace referencia a las personas, ya que son quienes tienen el contacto directo con los sistemas.

Esta fase se divide en cuatro procesos:

- **Proceso 1:** se recopila la siguiente información:
    - Niveles de seguridad de los activos de la organización.
    - Información de los riesgos.
    - Planes de mitigación con los que cuenta la organización.
- **Proceso 2:** se reúne información de las áreas operativas de la empresa u organización.
- **Proceso 3:** en esta fase el personal del departamento de TI, y el personal de planta de la organización son quienes participan, pues se recolecta información relacionada con

los requerimientos de seguridad de la organización, de los activos y de los planes de mitigación.

- **Proceso 4:** se evalúa la información recopilada durante los tres primeros procesos, dicha evaluación está a cargo del equipo de análisis, después de que se realizó la evaluación, se eligen los activos más importantes para la organización y a cada uno se les define un conjunto de requisitos y amenazas.

Fase 2. Análisis de la infraestructura.

En esta fase se evalúa la infraestructura física y tecnológicamente, y al igual que en la primera fase, se identifican las amenazas que las que pueda estar expuesta la infraestructura. La segunda fase de OCTAVE se divide en dos procesos:

- **Proceso 5:** el personal de TI trabaja junto con el equipo de análisis para identificar los componentes y sistemas críticos para los activos más importantes elegidos anteriormente.
- **Proceso 6:** durante esta fase, se tienen que evaluar los componentes identificados en el proceso anterior para detectar las vulnerabilidades con las que cuentan dichos componentes.

Fase 3. Análisis de riesgos.

En la última fase, se tiene que hacer una evaluación de todas las amenazas encontradas, además se tienen que identificar los riesgos a los que se expone la organización. Es posible que la organización tenga implementados controles de seguridad para minimizar dichos riesgos, sin embargo, si durante el análisis se detecta que dichas medidas no son suficientes pueden realizarse mejoras a los controles existentes para reducir el nivel de los riesgos, o también pueden crearse nuevos controles que satisfagan las necesidades de la organización. Esta fase se divide en dos procesos:

- **Proceso 7:** en este proceso se identifican los riesgos a los que pueden estar expuestos los activos, es decir, se hace un análisis de riesgos.
- **Proceso 8:** de definen las estrategias de protección para reducir los riesgos que se encontraron. Antes de ser ejecutadas, es necesario que los altos mandos las aprueben o hagan las correcciones necesarias.

OCTAVE es una metodología orientada a resultados, esto significa que con las acciones que se tomen se pueden alcanzar o incluso superar los objetivos planteados. Después de aplicar esta metodología por un lapso de dos o tres meses, la organización obtendrá un plan para mitigar los riesgos a largo plazo. Después de aplicarla de seis meses a un año se puede obtener un plan de mitigación bien detallado, asumiendo que la organización está siguiendo correctamente las recomendaciones de los estándares.

(Alemán Novoa & Rodríguez Barrera, 2021; De la Cruz, 2021; Ruge Pinzón, 2011)

5.5.1.2 MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas major conocida como MAGERIT es una metodología desarrollada por el Consejo Superior de Administración Electrónica del gobierno de España. Actualmente es mantenida por la Secretaría General de Administración Digital en conjunto con la Centro Criptológico Nacional. Esta metodología define la seguridad como el nivel de confianza que tienen los sistemas para resistir a las actividades ilícitas que ponen en riesgo la autenticidad, confidencialidad, integridad y disponibilidad de los datos de la organización, así como de los servicios que ofrece.

En la metodología MAGERIT, el analista de riesgos debe saber manejar los seis elementos básicos que considera esta metodología, los cuales son:

- Activos.
- Amenazas.
- Riesgo.
- Impacto.
- Vulnerabilidades.
- Salvaguardas (funciones, servicios y mecanismos).

MAGERIT implementa la gestión de riesgos dentro de un marco de trabajo, esto es muy importante, ya que va a permitir que se tengan en cuenta los riesgos que corre la organización al usar las TI en la toma de decisiones.

Los objetivos de esta metodología son:

- Hacer conscientes a los miembros de la organización acerca de la importancia de los riesgos y su gestión.
- Brindar un método que ayude a analizar los riesgos que surgen debido al uso de las TIC.
- Permitir que los riesgos sean identificados para crear un plan de mitigación oportuno y así mantenerlos controlados.
- Preparar a la organización para los procesos de:
    - **Evaluación:** permite saber qué tan confiable es un sistema de información.
    - **Certificación:** consiste en demostrar la capacidad del sistema para proteger la información que almacena, esto se hace mediante una serie de evaluaciones, por lo tanto, las evaluaciones originan las certificaciones, y algunas de las certificaciones tienen como objetivo las acreditaciones.
    - **Acreditación:** es un proceso que se sigue para determinar si un sistema puede formar parte de uno más grande.

- **Auditoría:** es un tipo evaluación que parte de un análisis de riesgos, como resultado, surge un informe donde se puede observar si las medidas de seguridad aplicadas cubren las necesidades identificadas, en caso de no ser así, se proponen medidas que ayuden a corregir o complementar la seguridad.

MAGERIT se compone de cuatro etapas:

Etapa 1. Planificación.

Se estudia la posibilidad de hacer un análisis y gestión de riesgos, asimismo, se define cuales son los objetivos y se identifican los medios materiales y humanos para realizarlo.

Etapa 2. Análisis de riesgos.

Se identifican y valoran los activos, también se obtiene una evaluación del riesgo y se realiza una estimación de los niveles de riesgo aceptables para la organización.

Etapa 3. Gestión de riesgos.

Se identifican los salvaguardas existentes que serán útiles para reducir los riesgos, dichos salvaguardas pueden ser funciones y servicios, de los cuales mediante la simulación de sus combinaciones se tienen que seleccionar los que ofrecen mayor nivel en la reducción de riesgos.

Etapa 4. Selección de salvaguardas.

Se diseña un plan para implementar los salvaguardas elegidos, también se hace una recopilación de la documentación obtenida durante el análisis y la gestión de riesgos, con lo cual se obtiene la documentación final del proyecto, posteriormente se presentan los resultados en diferentes niveles.

La metodología MAGERIT es muy útil para implementar medidas de mitigación que ayuden a controlar los riesgos, tiene como desventaja que es una metodología costosa, sin embargo, es muy completa para realizar los análisis de riesgos ya que, adicionalmente, prepara a la organización para la certificación, evaluación, acreditación y auditoría.

(Alemán Novoa & Rodríguez Barrera, 2021; Portal Administración electrónica, s. f.; Ruge Pinzón, 2011; Toro, 2015)

5.5.1.3 CRAMM – CCTA Risk Analysis and Management Method

El CCTA Risk Analysis and Management Method o Análisis de Riesgos y Método de Gestión, mejor conocido como CRAMM es una metodología para el análisis de riesgos, elaborada por el CCTA o Central Communication and Telecommunication Agency (Agencia Central de Informática y Telecomunicaciones) del Reino Unido en el año 1985. Esta metodología

proporciona información acerca del funcionamiento del sistema, también ayuda a identificar los activos que están más expuestos a los riesgos, para posteriormente implementar medidas que les ayuden a reducirlos. CRAMM proporciona integridad, confidencialidad y disponibilidad a los sistemas de información, esto lo logra realizando un análisis de riesgos cualitativo y cuantitativo, es decir, haciendo una evaluación mixta.

Para que el análisis de riesgos se realice de manera efectiva, y se obtenga un mejor resultado que asegure el funcionamiento continuo de la organización, deben considerarse los siguientes elementos:

- Vulnerabilidades.
- Riesgos.
- Amenazas.
- Contramedidas.
- Auditoría.

La metodología CRAMM tiene tres finalidades:

- Mejorar el nivel de seguridad de los sistemas de información.
- Justificar los costos que implica implementar medidas de seguridad.
- Demostrar la credibilidad de la información mediante los análisis realizados.

Para calcular los riesgos a los que se exponen los activos se usa una escala del 1 al 7, donde 1 significa que los requisitos de seguridad no son muy altos, mientras que 7 indica que se requieren medidas de seguridad elevadas.

CRAMM se divide en tres etapas:

Etapa 1. Establecimiento de objetivos de seguridad.

En esta primera etapa se definen de manera global los objetivos, es decir, se define el alcance, y se hace una identificación de los activos tangibles e intangibles para posteriormente evaluarlos y determinar cuáles son los activos más importantes y con esto se clasifican de acuerdo al impacto que generan en la organización.

Etapa 2. Análisis de riesgos.

Se identifican las amenazas y vulnerabilidades que podrían perjudicar al sistema, después de esto, se calcula el riesgo que tendría la organización si la amenaza se ejecutara.

En esta etapa, también debe considerarse el impacto que tendría la organización si su confidencialidad, integridad y disponibilidad se vieran afectadas.

Etapa 3. Identificación y elección de salvaguardas.

Se deben identificar las medidas de seguridad, cabe mencionar que CRAMM proporciona una biblioteca con una gran cantidad de contramedidas que pueden ser usadas por la organización. Después de haber identificado las medidas de seguridad de acuerdo a las necesidades que se quieren cubrir, deben aplicarse, para así obtener los riesgos residuales.

CRAMM es una metodología que puede aplicarse a cualquier tipo de sistema, además puede usarse en cualquier etapa del ciclo de vida de los sistemas de información para identificar los requisitos de seguridad y los requisitos de contingencia en caso de ser necesario. Adicionalmente, va a permitir que las organizaciones se preparen para su certificación de acuerdo con la ISO 27001.

(Alemán Novoa & Rodríguez Barrera, 2021; Ruge Pinzón, 2011)

5.5.1.4 EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité

La Expresión de las Necesidades e Identificación de los Objetivos de Seguridad, conocida como EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) es una metodología para analizar y gestionar riesgos promovida en Francia por la DCSSI o Direction Centrale de la Sécurité des Systèmes d'Information (Dirección Central de la Seguridad de los Sistemas de Información). EBIOS toma en cuenta los aspectos técnicos y los no técnicos, es decir, integra a las diferentes áreas de la organización y estudia el ciclo de vida del sistema desde su diseño hasta su mantenimiento.

Esta metodología puede ser adaptada a las necesidades específicas de la organización, tiene la capacidad de adaptarse a sistemas simples y complejos, así como a sistemas en proceso de diseño.

EBIOS consta de cinco fases:

Fase 1. Estudio del contexto.

Como primera fase, EBIOS realiza un estudio del contexto de la organización, es decir, estudia su historia y evolución para identificar los activos que tienen relación con la organización, como el hardware, software, redes, personal e infraestructura.

Fase 2. Expresar las necesidades de seguridad.

Todos los activos que fueron identificados en la primera fase requieren de medidas de seguridad diferentes, por lo que durante esta fase se evalúan las necesidades de dichos activos basándose en criterios previamente definidos, debe tomarse en cuenta que impacto tendría la organización si alguno de estos activos se viera afectado.

Fase 3. Estudio de las amenazas

Se identifican las amenazas y las formas de ataque a las que está expuesto cada uno de los activos. Para hacer esta identificación se tiene que tomar en cuenta el entorno de cada activo, ya que cada activo estará expuesto a diferentes tipos de amenaza y formas de ataque.

Fase 4. Expresar los objetivos de seguridad.

Se tienen que definir los riesgos a los que están expuestos los activos, es decir, hay que identificar las situaciones o escenarios peligrosos que al aprovecharse de las vulnerabilidades de los activos los afecten.

Los objetivos de seguridad a los que se refiere esta fase son los que permitirán cubrir las vulnerabilidades detectadas en los activos para disminuir los riesgos a los que se exponen. Cabe mencionar que hay que dar prioridad a los activos que son más críticos para la organización.

Fase 5. Determinar los requerimientos de seguridad.

Las personas encargadas de implementar la metodología EBIOS dentro de la organización deben detallar las funcionalidades esperadas de seguridad, esto para comprobar que dichas funcionalidades cubren por completo los objetivos de seguridad y probar que con los requisitos de seguridad especificados se alcanza el nivel de confianza necesario.

Finalmente, se puede observar que la metodología EBIOS puede adaptarse a las necesidades de seguridad de cada una de las organizaciones, además de que permite que las organizaciones tengan un mayor reconocimiento en sus labores relacionadas con la seguridad, esto se debe a que EBIOS es compatible con normas internacionales, como la ISO.

(Alemán Novoa & Rodríguez Barrera, 2021; DCSSI, 2004)

Tema 6. Entorno social, ética informática e impacto económico de la seguridad informática

6.1. Delito informático

Desde la creación del telégrafo en el siglo XIX, se interceptaban las comunicaciones para la transmisión de información falsa, esto indica que los delitos en las comunicaciones no se vinculan únicamente al surgimiento de las computadoras, es decir, este tipo de delitos han evolucionado para adaptarse a las tecnologías que surgen con el paso del tiempo.

En la década de los 60, surgieron los phreakers, que como se mencionó en el tema 3.3.1 eran un tipo de atacante que replicaban las frecuencias que utilizaba AT&T para realizar llamadas a larga distancia de manera gratuita.

En la década de los 70, es cuando surgieron las primeras acciones ilícitas relacionadas con las computadoras, durante esta época los delitos informáticos que más destacaban eran: el espionaje, la piratería de software, el sabotaje a las bases de datos y la extorsión.

A principios de la década de los 80, se instalaron teclados falsos en los cajeros automáticos para copiar la información de las tarjetas, y como una medida de seguridad se integraron los chips al plástico de éstas.

En la década de los 90, con la apertura global de internet, las industrias cinematográfica y discográfica enfrentaron muchos casos de violaciones a los derechos de autor, ya que comenzó la descarga e intercambio ilegal de música y películas protegidas con copyright, al mismo tiempo, se distribuían imágenes de pornografía infantil a través de internet.

El avance, el surgimiento de las nuevas tecnologías y el auge del internet, han provocado la creación de nuevas formas de delitos informáticos o ciberdelitos, donde los delincuentes informáticos hacen uso de herramientas electrónicas para acceder ilegalmente a un sistema, con el fin de dañar o destruir activos y/o sistemas para posteriormente, robar información, espiar el tráfico de la víctima o realizar estafas, entre otras acciones.

Los delitos informáticos, también conocidos como delitos cibernéticos o ciberdelitos, hacen referencia a comportamientos ilegales y no éticos haciendo uso de diferentes dispositivos electrónicos, software e internet, para acceder a información confidencial y usarla de manera maliciosa, con este tipo de acciones, las víctimas tienen distintos tipos de pérdidas, mientras que los delincuentes obtienen diferentes beneficios.

Cuando una persona u organización es víctima de un delito informático es complicado obtener pruebas que revelen la identidad del atacante, esto se debe a que el atacante puede estar en una ubicación remota llevando a cabo las acciones ilícitas, por lo que muchas veces las victimas conocen únicamente las acciones que llevó a cabo, pero no conocen al autor.

Actualmente, a través de internet se puede obtener mucha información como se ha visto en temas anteriores, es por ello que es importante conocer los tipos de delitos informáticos más comunes:

- **Sabotaje:** al realizar este tipo de ataques, el atacante pretende modificar o eliminar información de los dispositivos para evitar que éstos funcionen correctamente.
- **Espionaje:** las principales víctimas de este tipo de ataque son las empresas y organizaciones gubernamentales, los atacantes buscan obtener la información que almacenan en sus sistemas y hacerla pública, al hacer esto, activistas informáticos u otros tipos de delincuentes pueden aprovechar para realizar otros tipos de ataque.
- **Fraudes:** los atacantes usan diferentes métodos para obtener información personal y llevar a cabo actos ilegales, como la manipulación de información o el robo de identidad.
- **Piratería de software:** hace referencia a la distribución ilegal de software.
- **Acceso no autorizado:** como su nombre lo indica, es cuando el atacante viola las medidas de seguridad implementadas por la organización para acceder al sistema y posteriormente aprovechar la información para realizar diversas acciones.

Como se mencionó, las personas en general y organizaciones están expuestas a ser víctimas de un delito informático, sin embargo, hay medidas que pueden ayudar a minimizar el riesgo de convertirse en víctima de un delincuente informático, entre las cuales se encuentran:

- **Usar contraseñas seguras:** en el tema 3.2.1 se mencionaron las características que debe tener una contraseña para ser considerada segura. A modo de resumen, para crear una contraseña segura debe evitarse el uso de información personal, como nombres de usuario, el nombre de algún familiar o mascota y fechas de nacimiento, en su lugar, se debe usar una combinación de minúsculas, mayúsculas, caracteres especiales y números, asimismo es importante que en cada aplicación se tenga una contraseña diferente.
- **Estar atento al phishing:** hay que permanecer alerta a llamadas, mensajes, correos electrónicos o cualquier otro medio donde el delincuente informático pueda ponerse en contacto con la víctima, siempre hay que verificar que los remitentes sean auténticos antes de proporcionar información que pueda poner en riesgo la seguridad.
- **Usar antivirus:** el uso de antivirus y antimalware es fundamental para proteger los dispositivos y evitar que algún virus o malware se instale, arriesgando la seguridad de la víctima y la información almacenada en el dispositivo.
- **Usar VPN:** las VPN proporcionarán mayor seguridad al conectarse a la red, protegiendo la información que circula mediante ella.
- **Evitar el uso redes públicas:** este tipo de redes carecen de seguridad, por lo que la información que viaja a través de ellas es de fácil acceso para los delincuentes informáticos obteniendo información importante para después usarla en su beneficio.
- **Realizar copias de seguridad:** esto es de suma importancia, las copias de seguridad son útiles para que en caso de pérdida la información pueda ser restaurada evitando grandes pérdidas.
- **Cuidar la información que se comparte en internet:** hay que tener cuidado con los datos que se comparten a través de internet, en particular en las redes sociales, ya que

hay personas que suelen publicar información personal, la cual podría usar un delincuente para acceder a las cuentas de su víctima y realizar diferentes actividades delictivas, como robar su identidad, pedir algún tipo de remuneración a cambio de recuperar su información o no hacer públicos datos personales de la víctima, entre otros.

- **Evitar la instalación software de fuentes no confiables:** esto es porque el software puede albergar un virus o malware que puedan dañar al dispositivo dejándolo inservible o robar información sin que la víctima se dé cuenta.

El uso de internet proporciona grandes beneficios, sin embargo, hay que estar alerta a los riesgos que se pueden correr si no se toman las precauciones necesarias.

(BBVA, 2024; Cassou Ruíz, s. f.; Delgado Granados, s. f.; Loredo González & Ramírez Granados, s. f.; Revista Seguridad 360, 2021)

6.2. Marco legal mexicano

6.2.1. Acceso ilícito a sistemas

El acceso ilícito a sistemas, como su nombre lo indica, hace referencia a cuando algún individuo, sistema o proceso accede remota o directamente a un sistema sin tener autorización, también puede referirse a cuando el individuo accede más allá de donde tiene autorizado acceder, rompiendo o burlando las medidas de seguridad implementadas en el sistema.

En México, este delito está regulado en el Código Penal Federal también conocido como CPF, y se define como el acceso no autorizado a un sistema, burlando las medidas de seguridad, una vez que el delincuente está en contacto con la información puede realizar alguna otra actividad como copiar, modificar o eliminar el contenido de manera total o parcial, por lo que el CPF considera el acceso ilícito a sistemas como hacking informático.

En el CPF se encuentran definidas las sanciones para todos los que cometan este tipo delito, las sanciones dependen del:

- **Tipo de delito:** modificación, conocimiento, destrucción, copia o provocación de pérdida de información.
- **Tipo de dispositivo o sistema:** es decir, si es de propiedad de particulares, del Estado o de instituciones que integran el sistema financiero.
- **Quién cometió el delito:** es decir, si el delito fue cometido por algún servidor público, algún empleado o un funcionario de las instituciones que integran el sistema financiero.

Como ya se mencionó, las sanciones para este delito se encuentran definidas en el CPF, en el segundo libro, titulo noveno llamado “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática” este se encuentra dividido en dos capítulos, y es en el capítulo II donde se encuentra la regulación de este delito, denominado “Acceso Ilícito a Sistemas y Equipos de Informática”, artículos 211 bis 1 a 211 bis 7, los cuales se resumen a continuación:

- **Artículo 211 bis 1.** Considera la información de los dispositivos y sistemas de informática protegidos por mecanismos de seguridad.
  Quien sin autorización:
  - Modifique, destruya o provoque pérdida de información se le impondrán de seis meses a dos años en prisión y de cien a trescientos días de multa.
  - Conozca o copie información se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa.

- **Artículo 211 bis 2.** Considera la información de los dispositivos y sistemas de informática protegidos por mecanismos de seguridad pertenecientes al Estado.
  Quien sin autorización:

- Modifique, destruya o provoque pérdida de información se le impondrán de uno a cuatro años en prisión y de doscientos a seiscientos días de multa.
- Conozca o copie información se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.
- Conozca, obtenga, copie o utilice información almacenada en dispositivos, sistemas o medios de almacenamiento de seguridad pública se le impondrán de cuatro a diez años de prisión y multa de quinientos a mil días.
    - Si quien accedió ilegalmente es o fue un servidor público en una institución de seguridad pública además de la sanción mencionada, se le impondrá la destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Si la actividad llevada a cabo dificulta la impartición de justicia, la sanción será duplicada.

- **Artículo 211 bis 3.** Sanciona a quienes teniendo autorización realicen actividades indebidas en dispositivos y sistemas de informática pertenecientes al Estado.
  Quien indebidamente estando autorizado:
    - Modifique, destruya o provoque pérdida de información, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días de multa.
    - Copie información se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días de multa.
    - Obtenga, copie o utilice información almacenada en dispositivos, sistemas o medios de almacenamiento informáticos en materia de seguridad pública se le impondrán de cuatro a diez años de prisión y una multa de quinientos a mil días.
        - Si quien cometió el delito es un servidor público en una institución de seguridad pública, se le impondrá hasta una mitad más de la sanción mencionada, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

- **Artículo 211 bis 4.** Considera la información almacenada en dispositivos y sistemas informáticos protegidos por mecanismos de seguridad de las instituciones del sistema financiero.
  Quien sin autorización:
    - Modifique, destruya o provoque pérdida de información se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.
    - Conozca o copie información se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

- **Artículo 211 bis 5.** Sanciona a quienes teniendo autorización realicen actividades indebidas en dispositivos y sistemas de informática de las instituciones que integran el sistema financiero.
  Quien indebidamente estando autorizado:
  - Modifique, destruya o provoque pérdida de información se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.
  - Copie información se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa.

  Las sanciones mencionadas aumentarán la mitad, si quien realiza el delito es un funcionario o empleado de las instituciones que integran el sistema financiero.

- **Artículo 211 bis 6.** Menciona que las instituciones que integran el sistema financiero mencionado en los artículos 211 bis 4 y 211 bis 5 son las que se señalan en el artículo 400 bis del CPF.
  Las instituciones financieras son las que brindan productos y servicios financieros como los bancos, las cajas de ahorro, las aseguradoras y las afore.

- **Artículo 211 bis 7.** Menciona que las sanciones mencionadas aumentarán hasta en una mitad si la información que se obtuvo es utilizada en beneficio propio o ajeno.

(Código Penal Federal, 1931)

(Biblioteca del Congreso Nacional de Chile, 2014; Justia, 2020; Vilches Abogados, 2018)

6.2.2. Código Penal

Un Código Penal es un documento que define las acciones que son consideradas delito y las sanciones que deben aplicarse a quienes cometan alguno, sin importar si son personas físicas (un ser humano) o jurídicas (una entidad).

México actualmente cuenta con un total de 33 Códigos Penales, uno por cada una de las entidades federativas del país y un Código Penal Federal que puede aplicarse en toda la República Mexicana.

En el México colonial, el Código Penal que estuvo vigente fue el Derecho Penal Castellano, el cual estaba muy influenciado por la iglesia, así que era muy difícil diferenciar los conceptos de pecado y delito. Es bien sabido que la Guerra de Independencia en México terminó el 27 de septiembre de 1821, sin embargo, fue hasta el 28 de diciembre del año 1836 que España reconoció a México como una nación libre, soberana e independiente a través del tratado de Santa María – Calatrava, firmado por Miguel Santa María y José María Calatrava.

El 4 de octubre 1824 fue promulgada la primera constitución en México, ésta establecía un régimen político federal, es decir, reconocía a cada una de las entidades del país como soberana, esto hizo que cada una de las entidades tuviera su propio código penal.

El primer texto penal de México surgió en 1831 y fue el Bosquejo General de Código Penal para el Estado de México, sin embargo, no alcanzó a volverse ley, después, en 1835 se promulgó el Código Penal del estado de Veracruz, siendo este el primer Código Penal del país, tenía 759 artículos y se dividía en tres partes, sin embargo, seguían existiendo sanciones como la pena de muerte y se sancionaban los delitos contra la religión, los cuales estuvieron vigentes durante de la época colonial, y desaparecieron con la expedición del Código Penal de Veracruz de 1868.

El primer Código Penal para el Distrito Federal, actualmente Ciudad de México, fue promulgado en 1871, constaba de 1150 artículos y reaparecía la pena de muerte, misma que fue eliminada con el surgimiento del Código Penal para el Distrito Federal de 1929. Tan solo unos años más tarde, el 14 de agosto de 1931, en el Diario Oficial de la Federación se publicó el Código Penal para el Distrito Federal y Territorios Federales, el 23 de diciembre de 1974, por decreto cambió su nombre a Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en materia de Fuero Federal, y después, el 18 de mayo de 1999 su denominación cambió a Código Penal Federal, nombre con el que es conocido actualmente.

El Código Penal Federal, es aplicado a los delitos de caracter federal de la República Mexicana, con delitos de orden federal se hace referencia a todos aquellos delitos que afecten la salud, economía, patrimonio o la seguridad del país.

El CPF tiene 429 artículos, los cuales se encuentran divididos en dos libros:

- **Libro Primero:** contiene las normas generales, estas son las que se aplican a todos los delitos. Esta primera parte del CPF contiene seis títulos y el título preliminar, el cual define el ámbito de aplicación del CPF, es decir, se especifica que el CPF será aplicado en los delitos de orden federal cometidos en todo el país, así como las consideraciones sobre los delincuentes y los delitos cometidos, es decir, qué delitos se consideran como ejecutados dentro del país, así sean cometidos por delincuentes mexicanos o extranjeros, también se indica qué medidas se tomarán si se comete algún delito que no esté contemplado en el CPF.
- **Libro segundo:** contiene las normas especiales, es decir, se especifican las acciones que son consideradas delito, así como las sanciones que deberán imponerse a los delincuentes. Esta segunda parte del CPF contiene artículos transitorios, veintiséis títulos, entre los cuales se encuentran delitos contra:
    - La seguridad de la nación.
    - El derecho Internacional.
    - La dignidad de las personas.
    - La seguridad pública.
    - La salud.

- La economía pública.
- El ambiente y la gestión ambiental.

(Código Penal Federal, 1931)

Como se mencionó al inicio del subtema, los estados de la República Mexicana son soberanos y autónomos, por lo que cada uno cuenta con su propio Código Penal, esto tiene una gran desventaja, ya que hay acciones que no son consideradas como delito en algunas entidades, mientras que en otras sí, por lo que algunos delitos se quedan impunes, para evitar esto, es necesario impulsar la creación de un código penal nacional para castigar de la misma forma todos los delitos cometidos en el país, y no solo los delitos de orden federal como lo indica el CPF, sin embargo, para aprobar un código penal único se debería modificar la Constitución Política de los Estados Unidos Mexicanos, ya que es en este documento donde se reconoce a cada uno de los estados del país como soberanos y autónomos, o en dado caso, buscar una aprobación de todos los estados para la creación de este código penal único, lo cual resolvería los conflictos que hay entre los diferentes códigos penales del país, para que los delitos de orden federal y los delitos de orden común sean castigados de forma igualitaria en todo el país.

(Carmona Dávila, s. f.; Justia, 2023; LexGoApp, s. f.; Lozada León, 2017; Secretaría de la Defensa Nacional, s. f.; Trujillo, 2020)

6.2.3. Derechos de autor

Los derechos de autor, como su nombre lo indica, permiten al autor decidir qué se puede hacer con sus creaciones, es decir, si pueden divulgarse, mantenerse inéditas, comercializarse, heredarse o transferir los derechos de autor a otra persona para que ella decida qué hacer con la obra. El objetivo de estos es proteger las obras para evitar que éstas sean divulgadas o copiadas por otras personas sin dar el respectivo reconocimiento a los autores, es decir, protege los derechos de los autores respecto a sus creaciones.

En México, la primera ley dentro de este ámbito fue la Ley Federal sobre el Derecho de Autor, ésta fue promulgada el 31 de diciembre de 1947, después fue publicada en el Diario Oficial de la Federación el 14 de enero de 1948 y entró en vigor el 29 de enero de 1948, sin embargo, fue derogada por la Ley Federal del Derecho de Autor (LFDA) de 1996, publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996.

La LFDA se conforma de 238 artículos divididos en 12 títulos. El artículo 11 define los derechos de autor de la siguiente manera: “El derecho de autor es el reconocimiento que hace el Estado a favor de todo creador de obras literarias y artísticas”.

El artículo 13 de la LFDA indica los tipos de obras que protege esta ley, entre las cuales se encuentran:

- Obras literarias.
- Obras musicales con o sin letra.
- Caricaturas e historietas.
- Obras arquitectónicas.
- Programas de cómputo.
- Obras fotográficas.
- Enciclopedias o antologías.
- Bases de datos.

El artículo 14 de la LFDA indica los objetos que no pueden ser protegidos por los derechos de autor, entre los cuales se encuentran:

- Las ideas, fórmulas, soluciones, conceptos, métodos, sistemas, principios, descubrimientos, procesos e invenciones de cualquier tipo.
- Las letras, dígitos o colores aislados, a menos que su estilización sea tal que las conviertan en dibujos originales.
- Los nombres, títulos o frases aisladas.
- Las reproducciones o imitaciones sin autorización de escudos, banderas, emblemas de cualquier país, estado o municipio, ni las denominaciones, siglas, símbolos o emblemas de organizaciones internacionales gubernamentales o de cualquier otra organización reconocida oficialmente.
- Los textos legislativos, reglamentarios, administrativos o judiciales, así como sus traducciones oficiales. En caso de ser publicados, deberán apegarse al texto oficial y no conferirán derecho exclusivo de edición.
- El contenido informativo de noticias.
- La información de uso común, como los refranes, dichos, leyendas, hechos, calendarios y escalas métricas.

De acuerdo en la LFDA, los derechos de autor se dividen en:

- **Derechos morales:** están definidos en el capítulo II del título II, artículos 18 a 23. El artículo 18 indica que el autor es el único titular de los derechos morales de sus creaciones, y el artículo 19 menciona que el derecho moral se considera unido al autor y es:
    - **Inalienable:** es decir, nadie puede quitarle al autor los derechos sobre sus obras.
    - **Imprescriptible:** esto significa que los derechos de autor no acaban cuando el autor de la obra muere, estos perduran hasta cien años después de su muerte. En situaciones donde hay más de un autor, los cien años comienzan después de la muerte del último de los coautores.
    - **Irrenunciable:** es decir, que el autor o autores no pueden renunciar a la autoría de sus obras.

- **Inembargable:** significa que ninguna institución puede embargar el derecho del autor sobre sus obras.

En el artículo 21, se indica que los titulares de los derechos morales pueden:

- Determinar si su obra es divulgada y de qué forma, así como indicar si se mantiene o no inédita.
- Exigir respeto por su obra, anteponiéndose a cualquier deformación, mutilación o modificación.
- Retirar su obra del comercio.

- **Derechos patrimoniales:** se encuentran definidos en el capítulo III del título II, artículos 24 a 29. Este tipo de derechos indica que el autor puede explotar su obra y si permite a otros su explotación.

  De acuerdo con el artículo 26, el autor es el titular originario del derecho patrimonial y sus herederos o causahabientes se consideran titulares derivados. El artículo 26 bis indica que el autor y sus causahabientes podrán recibir regalías por la comunicación o transmisión pública de su obra.

  El artículo 27 indica que los titulares de los derechos patrimoniales entre las acciones que pueden autorizar o prohibir respecto a sus obras se encuentran:

  - La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico u otro similar.
  - La comunicación pública de la obra a través de:
    - La representación, recitación y ejecución pública en el caso de las obras literarias y artísticas.
    - La exhibición pública por cualquier medio o procedimiento en el caso de obras literarias y artísticas.
    - El acceso público por medio de la telecomunicación.
  - La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, incluyendo la transmisión o retransmisión de las obras por:
    - Cable.
    - Fibra óptica.
    - Microondas.
    - Vía satélite.
    - Cualquier otro medio conocido o por conocerse.
  - La divulgación de obras derivadas, en cualquiera de sus modalidades, tales como la traducción, adaptación, paráfrasis, arreglos o transformaciones.
- El artículo 29 indica que los derechos patrimoniales permanecerán vigentes:
  - Durante la vida del autor y cien años después de su muerte,
  - Si la obra tiene más de un autor, los cien años se contarán después de la muerte del último de los coautores.

- Cien años después de divulgadas.

En el título IV de la LFDA, capítulo IV llamado “De los programas de Computación y las bases de datos”, en los artículos 101 al 114, se habla del derecho de autor relacionado a los programas informáticos. Entre los artículos de este capítulo se encuentran:

- **Artículo 101:** define a un programa de computación como cualquier forma, lenguaje o código, de un conjunto de instrucciones que tiene una secuencia y una estructura determinada, con el propósito de que un dispositivo realice una tarea en específico.

- **Artículo 102:** menciona que los programas informáticos se protegen en cuanto a derechos de autor igual que las obras literarias, a excepción de aquellos programas informáticos que tengan como objetivo dañar a otros programas o dispositivos.

- **Artículo 106:** menciona que el derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:
  I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma.
  II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante.
  III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler.
  IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

- **Artículo 107:** menciona que las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedaran protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

- **Artículo 109:** también relacionada a las bases de datos, menciona que el acceso a información de carácter privado relativa a las personas contenida en las bases de datos, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.
  Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

- **Artículo 110:** está relacionado con el titular de los derechos patrimoniales de las bases de datos, quienes podrán autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma.
II. Su traducción, adaptación, reordenación y cualquier otra modificación.
III. La distribución del original o copias de la base de datos.
IV. La comunicación al público.
V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II de este artículo.

- **Artículo 112:** prohíbe la importación, fabricación, distribución y utilización de apartados o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos.

(Ley Federal del Derecho de Autor, 1996)

En México, la organización que se encarga de promover y proteger los derechos de autor es el Instituto Nacional del Derecho de Autor también conocido como INDAUTOR, este es un órgano desconcentrado adscrito a la Subsecretaría de Educación Superior (SES) de la Secretaría de Educación Pública (SEP).

Adicional a la LFDA, en el CPF, libro segundo, artículo vigesimosexto llamado “De los delitos en Materia de Derechos de Autor” sanciona los delitos llevados a cabo por delincuentes que infrinjan los derechos de autor, entre los cuales se encuentran:

- **Artículo 424:** impone una sanción de seis meses a seis años de prisión y de trescientos a tres mil días de multa:
    - A quien especule en cualquier forma con los libros de texto gratuitos distribuidos por la SEP.
    - Al editor, productor o grabador que produzca más ejemplares de los autorizados de una obra protegida por la LFDA.
    - A quien use con fines de lucro y sin autorización obras protegidas por la LFDA.

- **Artículo 424 bis:** impone una sanción de tres a diez años de prisión y de dos mil a veinte mil días de multa:
    - A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la LFDA con fines de especulación comercial sin autorización.
    - A quien fabrique con fines de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

    - A quien grabe, transmita o realice una copia total o parcial de una obra cinematográfica protegida, exhibida en una sala de cine u otros lugares sin autorización del titular del derecho de autor.

- **Artículo 427:** impone una sanción de seis meses a seis años y de trescientos a tres mil días de multa, a quien publique una obra substituyendo el nombre del autor por otro nombre.

- **Artículo 427 bis:** impone una sanción de seis meses a seis años de prisión y de quinientos a mil días de multa a quien con fines de lucro eluda sin autorización cualquier medida tecnológica de protección efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como autores de cualquier obra protegida.

- **Artículo 427 ter:** impone una sanción de seis meses a seis años de prisión y de quinientos a mil días de multa, a quien con fines de lucro fabrique, importe, distribuya, rente o de cualquier manera comercialice dispositivos, productos o componentes destinados a eludir una medida tecnológica de protección efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida.

- **Artículo 427 quárter:** impone una sanción de seis meses a seis años de prisión y de quinientos a mil días de multa a quien con fines de lucro ofrezca servicios al público destinados principalmente a eludir una medida tecnológica de protección efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como autores de cualquier obra protegida.

(Código Penal Federal, 1931)

Con lo anterior se puede comprender que es importante respetar los derechos de autor, no solamente para evitar la penalización correspondiente por el delito cometido, sino también para que los autores se sientan con la libertad de seguir creando y aportando con sus obras a la sociedad, teniendo la certeza de que su trabajo está protegido para evitar que otros lucren con sus aportaciones sin su autorización.

(Cofide, 2019; INDAUTOR, s. f.; Organización Mundial de la Propiedad Intelectual, s. f.; Presidencia de la República, 2013; UPAEP, s. f.)

6.2.4. Actualidad de la legislación sobre delitos informáticos

Como se ha estado mencionando en repetidas ocasiones, el uso de internet ha aumentado, esto se debe a los dispositivos electrónicos que existen actualmente, ya que es más fácil que la población se conecte a internet, esto tiene grandes ventajas, ya que se pueden realizar diferentes actividades, como tomar clases, trabajar a distancia, realizar pagos en la banca electrónica e incluso estar en contacto con personas lejanas por medio de las redes sociales, sin embargo, el uso de internet también trae desventajas, ya que los delincuentes informáticos aprovechan cuando los usuarios no ponen el suficiente cuidado al navegar por internet, quedando expuestos a ataques llevados a cabo por los ciberdelincuentes.

En la legislación mexicana se castigan algunos delitos informáticos, sin embargo, no se cuenta con una definición propia de delito informático, esto provoca que muchas acciones realizadas por criminales cibernéticos queden impunes, porque no se encuentran contempladas dentro de la legislación, y de acuerdo con el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos no se pueden sancionar actividades que no estén decretadas por alguna ley que sea aplicable al delito en cuestión.

Adicional al hecho de que no haya leyes que castiguen los delitos informáticos se suma el rápido avance de la tecnología en la actualidad, lo que causa que también haya una evolución agigantada en los nuevos tipos de delitos y cibercriminales que surgen, esto provoca que los nuevos delitos no se encuentren contemplados en la legislación. Con esto, se puede observar que México al no contar con leyes que sancionen los delitos informáticos se encuentra en un gran rezago si se habla de legislación sobre delitos informáticos.

Como se mencionó en el subtema 6.2.2, en México, cada una de las entidades cuenta con su propio Código Penal, y adicionalmente se cuenta con un Código Penal Federal, que sanciona únicamente los delitos de orden federal, al ser códigos penales diferentes, las denominaciones y sanciones de los delitos son diferentes, por lo que frecuentemente se recae en la impunidad antes mencionada, además de crear confusión en la población, ya que términos relacionados a los delitos informáticos frecuentemente vistos en los medios de comunicación como: phishing, ransomware, smishing o cyberbullying no están definidos en la legislación mexicana, en cambio, entre algunos de los delitos informáticos que se encuentran definidos en los diferentes códigos penales del país, incluyendo el CPF se encuentran:

- Delito equiparado al robo.
- Suplantación de identidad.
- Engaño telefónico.
- Delitos en materia de derechos de autor.
- Alteración o manipulación de medios de identificación electrónica.
- Acoso sexual.

- Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Con lo anterior se puede observar que es importante que en México exista una ley que castigue los delitos informáticos de igual manera en todo el país, principalmente para acabar con la impunidad, asimismo, es importante que exista una legislación en sincronía con las legislaciones internacionales, con el fin de evitar la confusión causada por la definición de los tipos de delitos informáticos en otros países.

En el año 2017, el gobierno mexicano creó la Estrategia Nacional de Ciberseguridad, cuyo objetivo es establecer acciones que dejen la población y a las instituciones públicas y privadas usar las TIC de manera responsable.

Desde el año 2018 se han propuesto 11 iniciativas de ciberseguridad en México, sin embargo, ninguna se ha concretado, lo que trae como resultado que muchos usuarios sean víctimas de ciberataques, entre ellos empresas e instituciones de gobierno, uno de estos casos es el hackeo a la Secretaría de Defensa Nacional (SEDENA) en 2022.

En septiembre del año 2022 se dio a conocer que un grupo hacktivista denominado “Guacamaya” hackeó los correos electrónicos del personal de la SEDENA desde julio de ese mismo año, dicho hackeo fue causado por una vulnerabilidad encontrada en el año 2021. Este ciberataque es considerado el de mayor impacto en México, ya que quedaron expuestos seis terabytes de información, situación que llevó a replantear la necesidad de tener una ley que se haga cargo de este tipo de deficiencias para que sean atendidas a tiempo y una situación como el hackeo a la SEDENA no se vuelva a repetir, ya que, por ejemplo, el CPF sanciona algunos delitos informáticos, pero no establece mecanismos para la gestión de riesgos que ayuden a fomentar cultura en el área de la informática.

Con el hackeo a la SEDENA, el Senado de la República y la Comisión de Ciencia y Tecnología e Innovación de la Cámara de Diputados propusieron la creación de una Ley Federal de Ciberseguridad, para esto, se hizo un análisis para comprender el rezago en el que se encuentra México en cuanto a la legislación en materia informática respecto a otros países.

Se estimaba que esta ley fuera publicada en diciembre del año 2022, sin embargo, hasta enero de 2024 no se tienen indicios de su publicación. Lo que se sabe de esta ley es que se consideran al menos cuatro planteamientos centrales, los cuales son:

- Crear una Agencia Nacional de Ciberseguridad.
- Garantizar la seguridad nacional a través la protección y defensa del espacio digital.
- Realizar pruebas pentesting cada año a instituciones públicas y privadas.
- Crear un marco legal que permita sancionar o tipificar los ciberataques.

Para que esta ley pueda ser cumplida correctamente, las instituciones públicas y privadas tendrán que contratar servicios de pentesting mínimo una vez al año, para que puedan detectar

vulnerabilidades y corregirlas antes de que un ciberdelincuente las aproveche y ponga en riesgo a la empresa o institución.

(Alvarado Andalón et al., s. f.; El Economista, 2022; Fuentes Rivera, 2023; Ochoa Serafín, 2023; Revista Fortuna, 2022)

6.2.5. Protección de la información

Como su nombre lo indica hace referencia al proceso de proteger la información que se tiene almacenada, asimismo, considera la opción de hacer las correcciones o actualizaciones necesarias en casos donde sea requerido, siempre y cuando se tenga la autorización necesaria del propietario de la información.

Como se ha visto anteriormente, la protección de información es necesaria para evitar filtraciones, alteraciones, daños o pérdidas de la misma, sin embargo, dentro de las estrategias para proteger la información se encuentran las estrategias de recuperación, estas son útiles cuando por algún motivo la información se daña o se pierde.

Durante el desarrollo de los diferentes temas se ha mencionado la importancia que tiene la protección de la información, haciendo referencia a la información que almacenan las organizaciones y empresas de manera general y que las hacen funcionar, sin embargo, este subtema tratará de la protección de información personal, ya que también es importante que se conozca la legislación existente en México sobre la protección de datos personales.

De acuerdo con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), los datos personales son los que identifican y diferencian a una persona, o, dicho de otra manera, se consideran como datos personales a toda aquella información mediante la cual se puede determinar la identidad de una persona, entre los cuales se encuentran:

- Nombre y apellidos.
- Correo electrónico.
- Número telefónico
- Fotografías.
- CURP (Clave Única de Registro de Población).
- Datos laborales.
- Fecha de nacimiento.
- Datos bancarios.
- Firmas (autógrafa y electrónica).

También se tienen los datos personales sensibles, estos se relacionan con aspectos más íntimos de la vida de las personas, entre los cuales se encuentran:

- Estado de salud.
- Información genética.
- Creencias.
- Orientación sexual.

Cada persona al ser dueña de su información tiene derecho a decidir sobre lo que se puede hacer con ella, es decir, cada uno puede decidir entre otras cosas si compartir o no su información, en caso de compartirla, decide con quién o quiénes lo hace y durante cuánto tiempo.

Muchas veces es necesario compartir información personal para adquirir servicios, sin embargo, si este tipo de información no se maneja correctamente puede traer muchos riesgos para el titular de la información, es por ello que la protección de datos personales es un derecho de los usuarios.

En México la protección de los datos personales en el contexto privado se encuentra regulada por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), mientras que la protección de datos personales en el contexto público se encuentra regulada por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares – LFPDPPP:** fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, esta ley tiene como objetivo regular la forma en la que los datos personales son tratados y permite a los titulares decidir libremente sobre el manejo de su información.
  La LFPDPPP es aplicable a las personas físicas o morales que hagan uso de los datos personales de las personas, por ejemplo, aplicaciones de streaming, compañías de teléfonos celulares, o tiendas en línea.
  Esta ley se compone de sesenta y nueve artículos, divididos en once capítulos y dos artículos transitorios.
- **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados – LGPDPPSO:** fue publicada en el Diario Oficial de la Federación el 26 de enero de 2017, su objetivo es establecer bases, principios y procedimientos que garanticen los derechos que tienen los titulares para proteger sus datos personales cuando están al alcance de los sujetos obligados.
  Con sujetos obligados se hace referencia a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, partidos políticos, fideicomisos y fondos públicos, es decir, esta ley es aplicable al tratamiento de datos personales hechos entre otros, por la Cámara de Diputados, la Suprema Corte de Justicia, o el Instituto Nacional Electoral (INE).
  Esta ley se compone de once títulos, ciento sesenta y ocho artículos y un artículo transitorio.

Estas leyes indican a los sujetos obligados y particulares que deben cumplir elementos que garanticen la seguridad de los datos personales, entre los cuales están:

Los sujetos obligados y particulares deben:

- Tener el consentimiento del titular de la información.
- Informar a los titulares el fin con el que es recolectada su información.
- Garantizar los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) de los titulares, estos están reconocidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos:
    - **Acceso:** se refiere a que los titulares tienen el derecho de acceder a su información personal que almacenan las dependencias.
    - **Rectificación:** hace referencia a que los titulares tienen el derecho de rectificar, corregir y actualizar su información en caso de ser necesario.
    - **Cancelación:** es decir, los titulares pueden pedir a las dependencias que sus datos sean cancelados o eliminados.
    - **Oposición:** se refiere a que el titular puede solicitar que sus datos personales no sean usados o dejen de usarse siempre y cuando tenga una causa legítima.

  Se habla de estos derechos en los capítulos III y IV de la LFPDPPP, y en el título tercero, capítulos I y II de la LGPDPPSO.

Asimismo, ambas leyes LFPDPPP y LGPDPPSO, mencionan que los responsables del tratamiento de los datos personales tienen que llevar a cabo los siguientes principios y derechos de protección:

1. **Licitud:** es decir, los sujetos obligados y particulares deben tratar los datos de los titulares de manera lícita y respetando lo que establece la legislación mexicana.
2. **Consentimiento:** hace referencia a que antes de que los sujetos obligados y particulares hagan uso de la información personal, los titulares deben dar su consentimiento, ya sea de forma tácita o expresa.
    a. **Consentimiento tácito:** es cuando el titular no expresa inconformidad después de haber recibido la información.
    b. **Consentimiento expreso:** es cuando el titular expresa su consentimiento de forma verbal, escrita o usando cualquier otro medio.
3. **Información:** indica que mediante un aviso de privacidad se le informará al titular la forma en la que sus datos serán administrados, dicho aviso de privacidad deberá contener la información necesaria usando un lenguaje comprensible con un diseño y una estructura clara.
4. **Calidad:** se refiere a que la información del titular deberá ser exacta, completa, pertinente, actualizada y correcta.
5. **Finalidad:** es decir, los datos del titular deberán ser tratados únicamente con la finalidad establecida en el aviso de privacidad.
6. **Lealtad:** se refiere a que los datos se recopilarán de forma lícita, es decir, no se pueden recopilar usando medios engañosos o fraudulentos.

7. **Proporcionalidad:** es decir, los sujetos obligados y particulares solo deberán tratar con los datos personales necesarios.
8. **Responsabilidad:** hace referencia a que los sujetos obligados y particulares son responsables del cómo son tratados los datos que recolectan, por lo que deben vigilar que se cumplan todos los principios involucrados en la protección de los mismos.

Estos principios se mencionan en el capítulo II de la LFPDPPP, y en el título segundo, capítulo I de la LGPDPPSO.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales mejor conocido como INAI es el organismo encargado de garantizar que los datos personales se traten adecuadamente. En el siguiente subtema se hablará más de este organismo.

(Adyen, 2022; INAI, s. f.-b, 2016; Ponce, 2023)

(Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010)

(Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, 2017)

6.2.6. Instituto Federal de Acceso a la Información

El Instituto Federal de Acceso a la Información también conocido como IFAI surgió el 25 de octubre del año 2002, la creación de este instituto tiene dos antecedentes muy importantes, el primero de ellos se remonta al año 2001, con el Grupo Oaxaca, un movimiento de académicos y activistas que luchaban por “el derecho a saber” y el segundo fue la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el 11 de junio del año 2002 en el Diario Oficial de la Federación, dicha ley entró en vigor el 12 de junio del mismo año.

El IFAI era el organismo encargado de hacer que las dependencias federales hicieran pública la información relacionada con el uso de recursos, y justificaran el porqué de sus acciones, lo cual era imposible hasta antes del surgimiento de este organismo, más tarde, a las funciones del IFAI se sumó la regulación de la protección y tratamiento de los datos personales.

Con la reformación del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos en el año 2007, se estableció como un derecho fundamental para los mexicanos el acceso a la información pública.

Después, en el 2010 con la aprobación de la LFPDPPP (subtema 6.2.5) el IFAI cambió de nombre, pasado a ser el Instituto Federal de Acceso a la Información y Protección de Datos.

Años después, en mayo de 2015 fue aprobada la Ley General de Transparencia y Acceso a la Información Pública, con la aprobación de esta nueva ley, el IFAI cambió su nombre a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o INAI.

La Ley General de Transparencia y Acceso a la Información Pública no solo trajo consigo el cambio de nombre a INAI, además trajo la renovación de la misión, visión y objetivos de la institución, volviéndose una institución autónoma, que vela por que el derecho a la información se cumpla, tal como se menciona en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.

El INAI es un organismo público autónomo cuyo objetivo es proteger el derecho de acceso a la información pública y la protección de los datos personales de los mexicanos, es decir, garantiza que las entidades federales proporcionen la información pública que los ciudadanos soliciten, asimismo, vela por el cumplimiento de los derechos ARCO de los ciudadanos (subtema 6.2.5), esto lo hace supervisando a instituciones para asegurarse que el trato a los datos personales que manejan sea acorde a lo establecido por la ley.

El INAI vela por el cumplimiento de las leyes LFPDPPP y LGPDPPSO, asimismo, impone sanciones a quienes no cumplan con sus obligaciones respecto al cuidado los datos personales, además brinda capacitaciones y apoyo técnico a los sujetos particulares y obligados si lo requieren.

Finalmente, se puede concluir que el INAI es un organismo que puede dar confianza a la población mexicana, como se ha estado viendo, la información personal es lo más valioso que tienen todas las personas, por lo que un mal uso podría arriesgar la vida, salud o integridad del titular, además de brindar transparencia en las decisiones tomadas por las instituciones federales, para que así la población pueda tener acceso a la información pública, lo cual era imposible antes del 2002.

(INAI, s. f.-c; V. Martínez, 2021; Maza, 2021; Notimex, 2015; Valenzuela, 2021)

6.3. Ley modelo (CNUDMI)

Cuando acabó la Segunda Guerra Mundial, representantes de 51 países se reunieron en la Conferencia de las Naciones Unidas la cual tuvo una duración de dos meses, realizándose del 25 de abril al 26 de junio de 1945 en San Francisco. Durante esos dos meses, se redactó y firmó la Carta de las Naciones Unidas, en la cual se esperaba que con la creación de la Organización Internacional de las Naciones Unidas se evitara otra guerra como la que se vivió entre los años de 1939 a 1946, y cuatro meses después el 24 de octubre del año 1945 las Naciones Unidas empezaron a existir de manera oficial.

México formó parte de los 51 países reunidos en la conferencia realizada de abril a junio de 1945, sus representantes fueron Ezequiel Padilla, Manuel Tello y Francisco Castillo Nájera, mismos que firmaron la Carta de las Naciones Unidas, y en 1947 fue creada la primera oficina de la ONU (Organización de las Naciones Unidas) en México.

Esta nueva organización tenía como objetivo conservar la paz y la seguridad internacional, alentar la formación las relaciones pacíficas y unir esfuerzos para que las naciones alcanzaran sus objetivos en común.

Actualmente, la ONU está conformada por 193 miembros, los cuales son:

Tabla 6.1. Miembros de la ONU.

No.	Miembro	Fecha de admisión	No.	Miembro	Fecha de admisión
1	Afganistán	19-11-1946	**98**	Kuwait	14-05-1963
2	Albania	14-12-1955	**99**	Lesotho	17-10-1966
3	Alemania	18-19-1973	**100**	Letonia	17-09-1991
4	Andorra	28-07-1993	**101**	Líbano	24-10-1945
5	Angola	01-12-1976	**102**	Liberia	02-11-1945
6	Antigua y Barbuda	11-11-1981	**103**	Libia	14-12-1955
7	Arabia Saudita	24-10-1945	**104**	Liechtenstein	18-09-1990
8	Argelia	08-10-1962	**105**	Lituania	17-09-1991
9	Argentina	24-10-1945	**106**	Luxemburgo	24-10-1945
10	Armenia	02-03-1992	**107**	Macedonia del norte	08-04-1993
11	Australia	01-11-1945	**108**	Madagascar	20-09-1960
12	Austria	14-12-1955	**109**	Malasia	17-09-1957
13	Azerbaiyán	02-03-1992	**110**	Malawi	01-12-1964
14	Bahamas	18-09-1973	**111**	Maldivas	21-09-1965
15	Bahrein	21-09-1971	**112**	Malí	28-09-1960
16	Bangladesh	17-09-1974	**113**	Malta	01-12-1964

17	Barbados	09-12-1966	**114**	Marruecos	12-11-1956
18	Belarús	24-10-1945	**115**	Mauricio	24-04-1968
19	Bélgica	27-12-1945	**116**	Mauritania	27-10-1961
20	Belice	25-09-1981	**117**	México	07-11-1945
21	Benin	20-09-1960	**118**	Micronesia	17-09-1991
22	Bhután	21-09-1971	**119**	Mónaco	28-05-1993
23	Bolivia	14-11-1945	**120**	Mongolia	27-10-1961
24	Bosnia y Herzegovina	22-05-1992	**121**	Montenegro	28-06-2006
25	Botswana	17-10-1966	**122**	Mozambique	16-09-1975
26	Brasil	24-10-1945	**123**	Myanmar	19-04-1948
27	Brunei Darussalam	21-09-1984	**124**	Namibia	23-04-1990
28	Bulgaria	14-12-1955	**125**	Nauru	14-09-1999
29	Burkina Faso	20-09-1960	**126**	Nepal	14-12-1955
30	Burundi	18-09-1962	**127**	Nicaragua	24-10-1945
31	Cabo Verde	16-19-1975	**128**	Níger	20-09-1960
32	Camboya	14-12-1955	**129**	Nigeria	07-10-1960
33	Camerún	20-19-1960	**130**	Noruega	27-11-1945
34	Canadá	09-11-1945	**131**	Nueva Zelanda	24-10-1945
35	Chad	20-09-1960	**132**	Omán	07-10-1971
36	Chequia	19-01-1993	**133**	Países Bajos	10-12-1945
37	Chile	24-10-1945	**134**	Pakistán	30-09-1947
38	China	24-10-1945	**135**	Palau	15-12-1994
39	Chipre	20-09-1960	**136**	Panamá	13-11-1945
40	Colombia	05-11-1945	**137**	Papua Nueva Guinea	10-10-1975
41	Comoras	12-11-1975	**138**	Paraguay	24-10-1945
42	Congo	20-09-1960	**139**	Perú	31-10-1945
43	Costa Rica	02-11-1945	**140**	Polonia	24-10-1945
44	Côte d'Ivoire	20-09-1960	**141**	Portugal	14-12-1955
45	Croacia	22-05-1992	**142**	Qatar	21-09-1971
46	Cuba	24-10-1945	**143**	Reino Unido de Gran Bretaña e Irlanda del Norte	24-10-1945
47	Dinamarca	24-10-1945	**144**	República Árabe Siria	24-10-1945
48	Djibouti	20-09-1977	**145**	República Centroafricana	20-09-1960
49	Dominica	18-12-1978	**146**	República de Corea	17-09-1991
50	Ecuador	21-12-1945	**147**	República de Moldova	02-03-1992
51	Egipto	24-10-1945	**148**	República Democrática del Congo	20-09-1960
52	El Salvador	24-10-1945	**149**	República Democrática Popular Lao	14-12-1955

53	Emiratos Árabes Unidos	09-12-1971	**150**	República Dominicana	24-10-1945
54	Eritrea	28-05-1993	**151**	República Popular Democrática de Corea	17-09-1991
55	Eslovaquia	19-01-1993	**152**	República Unida de Tanzanía	14-12-1961
56	Eslovenia	22-05-1992	**153**	Rumania	14-12-1955
57	España	14-12-1955	**154**	Rwanda	18-09-1962
58	Estados Unidos de América	24-10-1945	**155**	Saint Kitts y Nevis	23-09-1983
59	Estonia	17-09-1991	**156**	Samoa	15-12-1976
60	Eswatini	24-09-1968	**157**	San Marino	02-03-1992
61	Etiopía	13-11-1945	**158**	San Vicente y las Granadias	16-09-1980
62	Federación de Rusia	24-10-1945	**159**	Santa Lucía	18-09-1979
63	Fiji	13-10-1970	**160**	Santo Tomé y Príncipe	16-09-1975
64	Filipinas	24-10-1945	**161**	Senegal	28-09-1960
65	Finlandia	14-12-1955	**162**	Serbia	01-11-2000
66	Francia	24-10-1945	**163**	Seychelles	21-09-1976
67	Gabón	20-09-1960	**164**	Sierra Leona	27-09-1961
68	Gambia	21-09-1965	**165**	Singapur	21-09-1965
69	Georgia	31-07-1992	**166**	Somalia	20-09-1960
70	Ghana	08-03-1957	**167**	Sri Lanka	14-12-1955
71	Granada	17-09-1974	**168**	Sudáfrica	07-11-1945
72	Grecia	25-10-1945	**169**	Sudán	12-11-1956
73	Guatemala	21-11-1945	**170**	Sudán del Sur	14-07-2011
74	Guinea	12-12-1958	**171**	Suecia	19-11-1946
75	Guinea Bissau	17-09-1974	**172**	Suiza	10-09-2002
76	Guinea Ecuatorial	12-11-1968	**173**	Suriname	04-12-1975
77	Guyana	20-09-1966	**174**	Tailandia	15-12-1946
78	Haití	24-10-1945	**175**	Tayikistán	02-03-1992
79	Honduras	17-12-1945	**176**	Timor - Leste	27-09-2002
80	Hungría	14-12-1955	**177**	Togo	20-09-1960
81	India	30-10-1945	**178**	Tonga	14-09-1999
82	Indonesia	28-09-1950	**179**	Trinidad y Tobago	18-09-1962
83	Irán	24-10-1945	**180**	Túnez	12-11-1956
84	Iraq	21-12-1945	**181**	Turkmenistán	02-03-1992
85	Irlanda	14-12-1955	**182**	Türkiye	24-10-1945
86	Islandia	19-11-1946	**183**	Tuvalu	05-09-2000
87	Islas Marshall	17-09-1991	**184**	Ucrania	24-10-1945
88	Islas Salomón	19-09-1978	**185**	Uganda	25-10-1962
89	Israel	11-05-1949	**186**	Uruguay	18-12-1945

90	Italia	14-12-1955	**187**	Uzbekistán	02-03-1992
91	Jamaica	18-09-1962	**188**	Vanuatu	15-09-1981
92	Japón	18-12-1956	**189**	Venezuela	15-11-1945
93	Jordania	14-12-1955	**190**	Viet Nam	20-09-1977
94	Kazajstán	02-03-1992	**191**	Yemen	30-09-1947
95	Kenya	16-12-1963	**192**	Zambia	01-12-1964
96	Kirguistán	02-03-1992	**193**	Zimbabwe	25-08-1980
97	Kiribati	14-09-1999			

Información tomada de: https://www.un.org/es/about-us/member-states

En la década de 1960 comenzó a predominar el comercio internacional, en donde únicamente los documentos en papel eran válidos, esto no permitía que en las relaciones comerciales se hiciera uso de las tecnologías que iban surgiendo. Debido a esto, las Naciones Unidas decidieron participar activamente, y así fue como el 17 de diciembre del año 1966 la Asamblea General de las Naciones Unidas creó la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional o CNUDMI, también conocida como United Nations Commission on International Trade Law o UNCITRAL.

El objetivo de la CNUDMI es suprimir los impedimentos que hay en el comercio internacional, modernizando y unificando las reglas de la legislación comercial, además elabora textos relacionados al uso de las comunicaciones y firmas electrónicas.

Dentro de las labores de la CNUDMI se encuentra la elaboración de normas que permiten y facilitan el uso de los medios electrónicos dentro del comercio internacional. Una de estas normas es la Ley Modelo sobre firmas electrónicas, el objetivo de esta norma es establecer criterios de fiabilidad para que las firmas manuscritas y las firmas electrónicas sean equivalentes. En la actualidad, hay diferentes técnicas de autenticación que pueden sustituir las firmas manuscritas, la Ley Modelo se encarga de regular el trato jurídico de las firmas electrónicas y otros medios de autenticación electrónicos para que puedan ser ampliamente usados sin que haya dudas sobre su seguridad, para esto, establece criterios de fiabilidad donde se evalúan las responsabilidades y obligaciones de quien firma los documentos, de quien los recibe y de los intermediarios que intervienen en todo el proceso.

La otra norma es la Ley Modelo sobre el comercio electrónico, esta es una norma que contiene criterios que permiten facilitar el comercio usando medios electrónicos, estos criterios buscan que la información electrónica tenga el mismo valor que la información en papel, ya que esto hace que el comercio internacional sea más eficiente. Esta ley se encuentra disponible en cinco idiomas: árabe, chino, español, francés, inglés y ruso, además, se conforma de 17 artículos, los cuales se dividen en dos partes:

- **Parte I:** trata el comercio electrónico de forma general. Esta primera parte se encuentra dividida en 3 capítulos:

- **Capítulo 1. Disposiciones generales.**
  En este capítulo se introduce el concepto de *mensaje de datos,* este se define como “la información generada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax” (Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996, p. 4) El *intercambio electrónico de datos* o EDI (Electronic Data Interchange) hace referencia al intercambio de información entre computadoras.
- **Capítulo 2. Aplicación de los requisitos legales a los mensajes de datos.**
  Este capítulo hace referencia a la aplicación de los requisitos legales de los mensajes de datos, es decir, no se podrá negar su validez y en casos mayores, no se podrá negar la existencia de un contrato llevado a cabo mediante un mensaje de datos.
- **Capítulo 3. Comunicación de los mensajes de datos.**
  Este último capítulo hace referencia a la validez de los contratos celebrados mediante mensajes de datos, es decir, que ambas partes los acepten y además reconozcan los acuses de recibo, así como el tiempo y lugar de recepción y envío.

- **Parte II:** trata el comercio electrónico en áreas específicas. Solo consta de un capítulo:
  - **Capítulo I. Transporte de mercancías.**
    El capítulo se compone de dos artículos, los cuales son el artículo 16 y el artículo 17, donde se menciona como se regula el comercio electrónico en las áreas específicas.
    - **Artículo 16 – Actos relacionados con los contratos de transporte de mercancías:** este artículo aplica para los actos relacionados con el transporte de mercancías, dentro de los cuales se encuentran:
      a) Incluye indicar la marca, número, cantidad, peso y valor de las mercancías. Asimismo, se debe expedir un recibo y una confirmación de que la carga de mercancías fue completada.
      b) Se notifican las condiciones y cláusulas del contrato y se comunican las instrucciones al portador.
      c) Está relacionado con la autorización para la entrega de mercancías, también se incluyen las reclamaciones que llegaran a surgir sobre la entrega y la notificación de las pérdidas de las mercancías o de los daños que hayan sufrido.
      d) Se tienen que incluir otras notificaciones y/o declaraciones relacionadas al cumplimiento del contrato.
      e) Tiene que ver con que las mercancías sean entregadas a las personas designadas.

f) Está relacionado con la concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre las mercancías.
g) Se relaciona con la adquisición o transferencia de los derechos y obligaciones indicados en el contrato.

- **Artículo 17 – documentos de transporte:** este articulo está relacionado con el establecimiento de la singularidad de los mensajes de datos, es decir, los documentos que sean creados para llevar a cabo las diferentes acciones deberán ser únicos, de lo contrario no serán válidos a menos que se haga una cesión de derechos, un endoso o sus equivalentes.

(Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996)

Partes involucradas en las relaciones electrónicas.

El *mensaje de datos* es uno de los conceptos más importantes introducidos en la primera parte de la Ley Modelo de la CNUMDI sobre el comercio electrónico, sin embargo, adicionalmente en todo tipo de comunicaciones debe haber un remitente, un destinatario y un medio. En el artículo 2 de esta Ley Modelo, se definen los sujetos, los objetos y los medios involucrados en la relación electrónica:

- **Sujetos:** se incluyen al *iniciador*, al *destinatario* y al *intermediario*.
  - ***Iniciador:*** es quien que inicia el mensaje de datos, un iniciador puede ser un sistema o proceso que genere automáticamente los mensajes de datos sin que alguna persona intervenga, ya que dicho sistema o proceso, fue previamente programado para generar los mensajes de datos bajo el nombre de una persona. Un iniciador también puede ser una persona, sistema o proceso que genere un mensaje de datos con el único propósito de ser archivado.
  - ***Destinatario:*** es la persona, sistema o proceso con el que el iniciador se quiere comunicar.
  - ***Intermediario:*** es una persona, sistema o proceso que sirve de conexión entre el iniciador y el destinatario. Un intermediario puede retransmitir, formatear, traducir, certificar, autenticar o archivar los mensajes de datos, adicionalmente puede brindar servicios de seguridad en las operaciones electrónicas.
- **Medios:** hace referencia a los medios electrónicos mediante los cuales se puede enviar, recibir o archivar información en el comercio electrónico estos son llamados *sistemas de información,* dentro de estos se incluyen las redes de comunicaciones o el correo electrónico.

- **Objeto:** los objetos de las relaciones electrónicas son los *mensajes de datos,* que como ya se mencionó anteriormente, se entiende por *mensaje de datos* a la información que es enviada, recibida o archivada mediante los medios electrónicos.

A largo plazo, la Ley Modelo sobre el comercio electrónico tiene como objetivo adaptar sus criterios a las técnicas de comunicación que surjan con el paso del tiempo, esto porque los mensajes de datos se refieren a todo tipo de mensajes generados qué para enviarse, archivarse, etcétera, necesiten algún medio de comunicación electrónico.

(Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996)

(Embajada de México en Austria, 2016; Gobierno de Colombia, s. f.; Gobierno de México, s. f.; Naciones Unidas, s. f., 2022; PlataformaPYME, s. f.; Rojas Armandi, s. f.)

6.4. Legisladores internacionales

6.4.1. Legislación de Estados Unidos de América en Materia Informática

El Código de los Estados Unidos (United States Code) también conocido como USCODE o USC fue publicado en 1926, su primera edición se realizó en 1934, y desde entonces cada seis años la Oficina del Consejo de Revisión de Leyes de la Cámara de Representantes de los Estados Unidos se encarga de las ediciones principales, siendo la última en el año 2018, entre cada una de las ediciones se publican apéndices anuales para que la información esté actualizada cada año.

El USC se divide en 54 títulos generales, sin embargo, el título 53 está reservado para las pequeñas empresas, por lo que se dice que el USC se divide en 53 títulos generales, de los cuales, solamente se hablará acerca título 18 titulado Crimes And Criminal Procedure, artículo 47 Fraud and False Statements, específicamente de las secciones 1029 y 1030.

Sección 1029 – Fraud and related activity in connection with access devices.

Esta sección prohíbe el fraude y todo tipo de actividad delictiva haciendo uso de tarjetas de crédito, PINs, u otro tipo de identificadores, además indica que infringe la ley todo aquel que produzca, venda o use dispositivos electrónicos de comunicación con intenciones de cometer fraude y obtener productos y/o servicios de manera ilegal.

Actualmente, la sección 1029 cubre diez diferentes tipos de actividad delictiva, asimismo, indica las sanciones correspondientes al tipo de actividad.

United States Code [USC], Sección 1029 – Fraud and related activity in connection with access devices, (USA)

Sección 1030 – Fraud and related activity in connection with computers

La CFAA (Computer Fraud and Abuse Act) o Ley de Abuso y Fraude fue publicada en 1986, esta Ley es la que se usa comúnmente para castigar los delitos informáticos en Estados Unidos, actualmente, esta ley se encuentra en el título 18 del USC, artículo 47, en la sección 1030 titulada como *Fraud and related activity in connection with computers.*

Esta ley prohíbe todo tipo de acceso no autorizado o fraudulento a computadoras de interés federal, para causar algún tipo de daño, dentro de esta ley se encuentran protegidas, por ejemplo, las computadoras de los bancos. Además, esta ley menciona que la propagación de malware, como virus o gusanos es un delito. En otras palabras, esta ley protege a las computadoras y a los sistemas informáticos contra espionaje u otras formas de acceso ilegal.

Actualmente, esta ley considera que hay siete tipos de actividades delictivas y al igual que la sección 1029 impone sanciones a quienes violen dicha ley.

United States Code [USC], Sección 1030 – Fraud and related activity in connection with computers, (USA)

Adicionalmente hay leyes que fueron promulgadas para abarcar más áreas de seguridad, entre las cuales se encuentran:

Electronic Communications Privacy Act (ECPA)

La Ley de Privacidad en las Comunicaciones Electrónicas también conocida como ECPA que deriva del inglés Electronic Communications Privacy Act, fue promulgada en el año 1986, sin embargo, algunos años antes, en el año 1968 fue promulgada otra ley, llamada *Ley Ómnibus de Control del Crimen y Calles Seguras* esta ley se encontraba en el título 34 de la USC en la sección 10101.

La *Ley Ómnibus de Control del Crimen y Calles Seguras* se encargaba de proteger solamente las comunicaciones que podían ser escuchadas a través del oído humano, sin embargo, con el paso del tiempo, y los avances de la tecnología, surgió una nueva ley llamada *Ley de Privacidad en las Comunicaciones Electrónicas* o ECPA, esta fue promulgada en 1986 y ya abarcaba las nuevas tecnologías de comunicación electrónica, como la comunicación por correo electrónico, fax, entre otros.

En términos generales, esta ley prohíbe:

- Grabar o interceptar las comunicaciones sin previa autorización de las partes involucradas o sin que haya alguna orden del tribunal de por medio.
- Publicar el contenido de las comunicaciones sin autorización.
- Usar el contenido de dichas comunicaciones para acusar a alguien de algún crimen.

Dentro de una organización, la ECPA le permite a los empleadores leer, escuchar y borrar mensajes que son enviados y recibidos a través de los sistemas electrónicos propios de la organización, sin embargo, la ECPA señala que los empleadores deberán hacer saber a los empleados mediante un documento cuales son las reglas que deben seguir al momento de usar los medios electrónicos de comunicación pertenecientes a la organización y lo empleados deberán firmar dicho documento, como prueba de que conocen las reglas que deben seguir.

Actualmente la ECPA se divide en tres partes y está definida en el título 18 de la USC:

- **Artículo 119. Wire and Electronic Communications Interception and Interception of Oral Communications – Secciones 2510 a 2523:** esta parte de la norma señala que es ilegal interceptar y/o divulgar el contenido de las comunicaciones ya sean orales o electrónicas, asimismo, indica que es ilegal usarlas como prueba para acusar a alguien o usarlas como evidencia.

(United States Code, Titulo 18. Secciones 2510 a 2523)

- **Artículo 121. Stored Wire and Electronic Communications and Transactional Records Access – Secciones 2701 a 2713:** esta parte de la norma protege la privacidad de los archivos que se encuentran en sistemas que son usados para transmitir o almacenar información, un ejemplo es el contenido de los sistemas de los proveedores de servicios, además, indica que es ilegal acceder a algún sistema intencionalmente para obtener información y evitar o alterar el acceso a alguna de las comunicaciones electrónicas que alberga dicho sistema.
  (United States Code, Título 18, Secciones 2701 a 2713)
- **Artículo 206. Pen Registers and Trap and Trace Devices – Secciones 3121 a 3127:** esta última parte de la norma prohíbe a las entidades gubernamentales instalar algún tipo de mecanismo que capture la información relacionada con las comunicaciones electrónicas, como el número marcado o el origen de las comunicaciones, a menos que cuenten con una orden judicial.
  (United States Code, Título 18, Secciones 3121 a 3127)

Finalmente, cabe mencionar que está ley fue modificada a raíz de los acontecimientos terroristas ocurridos el 11 de septiembre del año 2001, ya que surgió la Ley Patriota de Estados Unidos.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act – USA Patriot Act

La Ley de Unión y Fortalecimiento de Estados Unidos mediante la Provisión de las Herramientas Necesarias para Interceptar y Obstruir el Terrorismo o mejor conocida como *Ley Patriota* o USA Patriot Act fue promulgada en octubre de 2001, pocos días después de los atentados terroristas ocurridos el 11 de septiembre de ese mismo año.

Esta ley fue creada con el objetivo de dar más autoridad al gobierno para la obtención de información de las personas y organizaciones con el fin de mejorar la seguridad nacional e impedir que en un futuro eventos similares ocurrieran. La Ley Patriota modificó 15 estatutos federales, dentro de los cuales se encuentran la CFAA y la ECPA, leyes de las cuales ya se habló con anterioridad.

Dentro de las acciones que esta ley permite para aumentar la seguridad nacional se encuentran:

- Permitir a los agentes federales las escuchas telefónicas, para la investigación de delitos vinculados con el terrorismo, y así localizar a personas sospechosas de llevar a cabo actividades terroristas.
- Permitir que sean usadas órdenes de registro de notificación diferida, esto para evitar que las personas sospechosas sepan que están siendo investigadas.
- Mejorar el intercambio de información entre las organizaciones gubernamentales y policiales, con el propósito de conseguir información de forma más rápida y ágil.

- Permitir que haya castigos más duros para las personas condenadas por la realización de actividades terroristas, así como la implementación de castigos para las personas que los estén cubriendo.

(BJA, s. f.; Borghello, s. f.; CaseGuard, 2022a, 2022b; Colorado Ángel & Torres Baquero, 2015; GovInfo, s. f.; National Association of Criminal Defense Lawyers, s. f.; Rojo García, 2022; Spiegato, 2021b; Vaquero, 2020)

6.4.2. Legislación de Australia en Materia informática

El Attorney General's Department o Departamento del Fiscal General es el encargado de únicamente administrar y aplicar las leyes del sistema legal australiano, cabe mencionar que no investiga los delitos, adicionalmente, desde el año 2019 también se ha encargado de dirigir las relaciones laborales de dicho país.

Entre las leyes que administra relacionadas con materia informática se encuentran:

- Telecommunications (Interception and Access) Act 1979 o Ley TIA (Ley de Acceso e Interceptación de Telecomunicaciones).
- Surveillance Devices Act 2004 o Ley SDA (Ley de Dispositivos de Vigilancia).

A continuación, se hablará de cada una de ellas.

Telecommunications (Interception and Access) Act 1979.

También conocida como TIA Act o Ley TIA, se encarga de proteger la privacidad de las comunicaciones, esta ley considera como delito que se accedan o intercepten comunicaciones privadas sin que se las partes involucradas en la misma tengan conocimiento o sin que se cuente con una orden del tribunal.

Para brindar una mayor seguridad, y que las leyes de seguridad nacional se apliquen correctamente, las agencias de seguridad tienen permitido interceptar comunicaciones, acceder a comunicaciones almacenadas e incluso difundir datos, esto para realizar investigaciones y posteriormente pueden solicitar una orden al tribunal. Otro de los casos en donde las agencias de seguridad pueden acceder a las comunicaciones sin tener una orden es en situaciones de emergencia.

La ley TIA proporciona un marco legal para que algunos miembros de las agencias con previa autorización puedan solicitar a los proveedores información sobre alguna comunicación en tiempo real o una comunicación almacenada que aporte información sobre los delitos graves o asuntos relacionados con la seguridad nacional.

(Australian Goverment, s. f.)

Surveillance Devices Act 2004.

También conocida como SDA Act o Ley SDA tiene por objetivo regular el uso de dispositivos de vigilancia, pero no contiene criterios que prohíban su uso. La ley SDA complementa las leyes de dispositivos de vigilancia de los estados, ya que permite que se obtengan órdenes para investigar delitos.

La ley SDA cubre diferentes aspectos, entre los cuales se encuentran:

- **Dispositivos de vigilancia de datos:** prohíbe la instalación y uso de dispositivos de vigilancia de datos que registren o monitoreen la entrada y/o salida de información de dispositivos electrónicos sin autorización del propietario, de quien use el dispositivo o en dado caso, sin que se cuente con una orden judicial.
- **Dispositivos de escucha:** prohíbe que se escuche, grabe o monitoree una conversación privada, sea o no participante en ella.
  Para que una conversación pueda ser escuchada, grabada o monitoreada, todas las partes involucradas deben dar su aprobación. También no aplica como delito si el dispositivo de escucha no se usa con el propósito de publicar la conversación con personas ajenas a la misma.
- **Dispositivos de vigilancia óptica:** prohíbe la instalación o uso de dispositivos de vigilancia ópticos en instalaciones, vehículos o cualquier otro lugar donde se pueda observar la realización de actividades sin que se tenga el consentimiento del propietario o sin que se tenga una orden judicial.
- **Dispositivos de seguimiento:** prohíbe la instalación o uso de dispositivos de seguimiento para determinar la ubicación geográfica de una persona sin su autorización, también prohíbe los dispositivos de seguimiento en objetos sin que se tenga la autorización del dueño o de quien posea el control de dicho objeto. En ambos casos, es posible su instalación y uso si se tiene una orden judicial o si se hace con propósitos legales.

La SDA también cubre otros aspectos, entre los cuales se encuentran:

- **Publicación de conversaciones privadas o grabaciones de actividades:** indica que no se puede publicar una conversación privada, una actividad, o registro de una actividad realizada, la ley no aplica si la publicación tiene relación con una fiesta o si todas las partes involucradas están de acuerdo con su publicación.
- **Fabricación, suministro y posesión de dispositivos de escucha:** indica que es ilegal fabricar, poseer o proveer dispositivos de escucha, de vigilancia óptica o de datos y de dispositivos de seguimiento, cuyo propósito sea ser usados sin las autorizaciones necesarias.

(Surveillance Devices Act 2007, 2022)

(Miralis, s. f.; Mundo a world of experts, s. f.; Notes De Seguretat, 2022)

6.4.3. Legislación de España en Materia Informática

El Boletín Oficial del Estado, también conocido como BOE es un diario donde se publican las leyes y los comunicados de manera oficial en España, hasta que las leyes son publicadas en este diario es cuando entran en vigor.

El BOE se divide en cinco secciones, las cuales son:

- Sección I. Disposiciones generales.
- Sección II. Autoridades y personal.
- Sección III. Otras disposiciones.
- Sección IV. Administración de justicia.
- Sección V. Anuncios.

La Agencia Estatal Boletín Oficial del Estado o AEBOE es una organización pública que depende del Ministerio de Presidencia de la AEBOE es la organización que publica, imprime y difunde todo lo que se encuentra en el BOE, de igual manera se encarga de administrar el BOE de manera electrónica.

En el BOE también se encuentran publicaciones relacionadas con la legislación informática, como el Código de Derecho de la Ciberseguridad el cual contiene normas relacionadas con la protección del ciberespacio, entre las cuales se encuentran:

- **Ley 34/2002 de 11 de julio. Servicios a la Sociedad de la Información y Comercio Electrónico.**
  Se encarga de regular la actividad económica realizada a través de internet. Establece criterios que las empresas y organizaciones que ofrecen productos y/o servicios en internet deben seguir para brindar una experiencia de compra segura.
  Algunos de los propósitos de esta ley son:
  - Fomentar la creación de empleos en el ámbito digital.
  - Promover la economía en el ámbito digital.
  - Establecer un marco legal que satisfaga las necesidades de los vendedores, prestadores de servicios y usuarios.

  (Ley 34/2002 de 11 de julio. Servicios a la Sociedad de la Información y Comercio Electrónico, 2002).

- **Ley 9/2014 de 9 de mayo. General de telecomunicaciones.**
  Con esta ley se pretende crear un ambiente de competencia efectiva en internet para la prestación de servicios. Entre los objetivos de esta ley se encuentran:
  - Desarrollar la economía digital.
  - Impulsar y desarrollar el empleo digital.
  - Promover el desarrollo de las telecomunicaciones y servicios digitales.

- Permitir que se desarrollen productos de telecomunicaciones.
- Hacer más fácil el acceso a la comunicación electrónica a los usuarios con discapacidades.

(Ley 9/2014 de 9 de mayo. General de telecomunicaciones, 2014)

- **Ley 25/2007 de 18 de octubre. Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.**

  El objetivo de esta ley es regular la conservación de los datos que generan los usuarios en las comunicaciones electrónicas, asimismo, indica que los proveedores de servicios deben proporcionar los datos solo a los agentes autorizados que presenten una orden judicial cuyos fines sean investigación, detección o enjuiciamiento de los delitos que contempla el Código Penal.

  Esta ley especifíca que deben conservarse los datos necesarios para:

  - Rastrear el origen de una comunicación.
  - Rastrear el destino de una comunicación.
  - Determinar la fecha, hora y duración de la comunicación.
  - Identificar el tipo de comunicación.
  - Identificar el tipo de equipo con el que se realizó la comunicación.
  - Localizar la ubicación del equipo con el que se realizó la comunicación.

  (Ley 25/2007 de 18 de octubre. Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, 2007)

- **Ley orgánica 3/2018 de 5 de diciembre. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).**

  Esta es considerada la norma de referencia para la protección de datos en España, entró en vigor el 6 de diciembre de 2018 y sustituyó a la Ley Orgánica 15/1999.

  La LOPDGDD define criterios para la protección de datos por parte de las organizaciones, por lo que se dice que esta ley protege la privacidad e integridad de los usuarios. Asimismo, contiene criterios que deben seguir los usuarios para que cuando proporcionen información personal lo hagan de manera segura.

  Esta ley considera como información personal a aquellos datos que permitan identificar a una persona, sin importar si es en texto, imágenes, video o audio. Hay algunos datos que no se consideran información personal como el nombre de la persona o el correo electrónico, sin embargo, datos relacionados con la religión o salud personal si son considerados información personal.

  Esta ley también incluye un apartado para la información de personas fallecidas. Si el fallecido indicó que hay una persona a la cual se le puede entregar su información personal, esta persona puede solicitarla y se le entregará, sin embargo, si el fallecido indicó que nadie puede obtener su información, esta no se entrega a nadie.

(Ley orgánica 3/2018 de 5 de diciembre. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, 2018).

(AEBOE, s. f.; Ciberseguridad, s. f.-d; Y. Fernández, 2020; Grupo Atico34, 2023)

6.4.4. Legislación de Canadá en materia informática

El 13 de abril del año 2000 surgió la Ley PIPEDA o Personal Information Protection and Electronic Documents Act, en español conocida como Ley de Protección de Información Personal y Documentos Electrónicos de Canadá, esta regula las acciones que puede llevar a cabo una empresa del sector privado sobre la información personal que manejan.

De acuerdo con la ley PIPEDA, las empresas deben garantizar la confidencialidad de la información sin importar en que formato se encuentre, debido a esto, entre la información personal que protege se encuentra la radiodifusión, el sector de la salud y el comercio electrónico.

Dentro de las medidas que se pueden implementar para que se pueda garantizar la confidencialidad de la información se incluyen:

- **Medidas físicas:** restringir el acceso a las instalaciones, para que solo accedan las personas con autorización, además de instalar sistemas de video vigilancia o alarmas.
- **Medidas lógicas:** contraseñas en los dispositivos, cifrado de información tanto enviada como almacenada, instalación de actualizaciones y parches de seguridad.

Para que las organizaciones recopilen, usen o divulguen información personal deben contar con la autorización de las personas y dicha recopilación debe realizarse usando medios legales, la ley PIPEDA también indica que las organizaciones o empresas no pueden negar un producto o servicio que el cliente desee adquirir aun cuando no permita que su información personal sea recopilada la ley solo permite negar la adquisición de productos y/o servicios en situaciones en las que la información personal sea necesaria para realizar la transacción.

Tomando en cuenta lo anterior, la ley PIPEDA brinda a las personas derechos sobre su información personal cuando es recopilada, entre los cuales se encuentran:

- Preguntar los motivos por los cuales la empresa u organización necesita recopilar, usar o divulgar su información.
- Obtener acceso a su información, así como solicitar correcciones en caso de ser necesario.
- Presentar una queja si la persona nota que la empresa u organización está haciendo un mal uso de su información o si sus derechos de privacidad no están siendo respetados.

Esta ley también autoriza que la información personal usada y/o divulgada sin consentimiento proteja la privacidad de las personas y solo se use en ciertas situaciones, dentro de las cuales se encuentran:

- Uso con fines periodísticos, artísticos, literarios, estadísticos, de estudio o de investigación.
- Información que está disponible públicamente.
- Una empresa u organización considera que la información podría ayudar a investigar el incumplimiento de una ley.
- La persona está en una situación de emergencia, donde su salud, su vida o su seguridad se ve amenazada.

(Thales, s. f.; Tyas Tunggal, 2023)

(Personal Information Protection and Electronic Documents Act, 2019)

6.4.5. Legislación de Venezuela en materia informática

El 30 de octubre de 2001 en la gaceta oficial de la República Bolivariana de Venezuela No. 37.313 fue publicada la Ley Especial contra Delitos Informáticos, sin embargo, entró en vigor un mes después, el día 30 de noviembre de 2001.

Esta ley tiene como propósito proteger los sistemas de tecnologías de información, para prevenir los delitos informáticos y sancionar aquellos delitos que se lleguen a cometer sobre el sistema o alguno de sus componentes, asimismo sanciona los delitos que se cometan usando tecnologías de información.

La Ley Especial contra Delitos Informáticos consta de 33 artículos divididos en cuatro títulos:

Título I. Disposiciones generales

Se muestra el objetivo de la ley, así como un glosario de términos, dentro de los cuales se incluyen:

- Tecnología de información.
- Datos.
- Sistema.
- Procesamiento de datos o de información.
- Seguridad.
- Virus.
- Contraseña.
- Mensaje de datos.

También se muestra lo que ocurre con los delitos extraterritoriales o cuando los delitos son cometidos por personas jurídicas.

Título II. De los delitos.

Consta de cinco capítulos, donde cada uno indica un tipo de delito considerado por esta ley:

- Capítulo I. De los delitos contra los sistemas que utilizan tecnologías de información.
- Capítulo II. De los delitos contra la propiedad.
- Capítulo III. De los delitos contra la privacidad de las personas y de las comunicaciones.
- Capítulo IV. De los delitos contra niños, niñas y adolescentes.
- Capítulo V. De los delitos contra el orden económico.

Título III. Disposiciones comunes.

Menciona como es que las sanciones para castigar delitos informáticos pueden aumentar si se detecta que para llevar a cabo el delito se hizo uso indebido de contraseñas o se obtuvieron abusando de los privilegios que se tienen como integrante de la organización.

Título IV. Disposiciones finales.

Indica que la ley entrará en vigor 30 días después de su publicación en la gaceta, además, menciona que fue dada, firmada y sellada en el Palacio Federal Legislativo el 4 de septiembre del año 2001.

(Venfort, 2019)

(Ley Especial contra los Delitos Informáticos, 2001)

6.5. Ética informática

6.5.1. Concepto de ética informática

Antes de definir el concepto de ética informática, hay que definir el concepto de *ética*. La palabra *ética* proviene del griego *ethos* que significa carácter o comportamiento.

Es común que muchas personas confundan los significados de ética y moral, o incluso lleguen a creer que son lo mismo, sin embargo, esto no es así. La moral es objeto de estudio de la ética y puede verse como un conjunto de normas y valores que son aceptados en una sociedad y que indican lo que está bien y lo que está mal dentro de esa sociedad.

Por otro lado, la RAE (Real Academia Española) define a la ética como un *"conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida".* La ética como rama de la filosofía estudia los actos conscientes, buenos y malos de los seres humanos. Es decir, la ética estudia la conducta humana al mismo tiempo que establece reglas que indican como es que debería ser el comportamiento humano en la sociedad.

Con el paso del tiempo y tomando en cuenta los avances tecnológicos es cómo surge la ética informática, esta puede definirse como la disciplina que analiza los problemas éticos que tienen origen en la creación de las TIC, es decir, analiza los problemas éticos que surgen gracias al uso malicioso que se le da a las TIC, con el propósito de perjudicar a los demás.

El origen de la ética informática data de la década de los setenta, ya que fue en esa época donde se comenzó a hacer un mayor uso de las computadoras, y con el paso del tiempo también surgieron nuevas tecnologías que trajeron como consecuencia los delitos informáticos, de ahí surgió la necesidad de crear principios éticos que rigieran el uso de los dispositivos electrónicos.

La ética informática tiene un papel muy importante tomando en cuenta que actualmente vivimos en un mundo digital, donde muchas de las actividades cotidianas hacen uso de dispositivos de TIC, por lo que dentro de la ética informática se incluye el manejo de dichos dispositivos, así como el manejo de la información, con todos los avances tecnológicos también es más fácil acceder a información y/o recursos almacenados en internet, por lo que es necesario que todos los usuarios se rijan por valores éticos que ayuden a preservar su seguridad y la de los demás.

Otros de los aspectos que abarca la ética informática son los efectos que tienen estos dispositivos en la sociedad, como se mencionó en el tema 2.2, las TIC tienen un gran impacto en el calentamiento global, ya que representan el 4% de las emisiones de gases de efecto invernadero, previendo que para el año 2025 este porcentaje aumente al 8%, además se debe tomar en cuenta la contaminación que se genera por los desechos informáticos.

En un informe elaborado por varias agencias de la ONU, se prevee que anualmente se producen 50 millones de toneladas de residuos eléctricos y electrónicos, de los cuales se reciclan

correctamente solo el 20%, por lo que la ética informática también abarca dichos efectos para buscar soluciones que minimicen el impacto negativo en el medio ambiente, como la tecnología verde, también mencionada en el tema 2.2.

Considerando lo anterior es posible darse cuenta de la importancia que tiene la ética informática, por lo que en el subtema 6.5.3 titulado “Contenidos de la ética informática” se profundiza en otros aspectos, tales como los principios y objetivos de la ética informática, también se proporciona información adicional para comprender de una mejor manera el concepto de ética informática y entender por qué actualmente es útil para regular el uso de los dispositivos de TIC.

(Arcila et al., 2009; Euroinnova Business School, s. f.; Normativa y Regulación Informática, 2015; Noticias ONU, 2019; Responsaibilidad Social Empresarial y Sustentabilidad, 2022; Silva & Espina, 2006)

6.5.2. Códigos deontológicos en informática

El término *deontología* fue acuñado por el filósofo Jeremy Bentham en 1889 en su obra *Deontology or the Science of Morality* (Deontología o ciencia de la moralidad), para Bentham las acciones que comprende la deontología no están controladas por algún sistema de normas vigente en un lugar determinado, sin embargo, dichas acciones deben realizarse de tal manera que produzcan beneficios a la sociedad. En este sentido, la deontología puede entenderse como el conjunto de principios, deberes y reglas que guían la conducta profesional.

Por otro lado, un código deontológico es un documento que contiene un conjunto de valores, normas y criterios que deberán seguir los profesionales en el desarrollo de sus funciones. Asimismo, define pautas para que los profesionales realicen dichas funciones de forma ética, y también se establecen sanciones para aplicarlas a los profesionales que no realicen su trabajo de acuerdo a los criterios previamente establecidos.

De manera regular, los códigos deontológicos abarcan lo siguiente:

- Objetivo de la profesión.
- Deberes generales de la profesión.
- Deberes específicos en situaciones especiales.
- Deberes respecto a los compañeros de profesión.
- Prohibiciones.

Todo lo que se recoge en el código deontológico, se encuentra aprobado por los colegios profesionales, estos son asociaciones cuyos miembros ejercen una misma profesión, y además de elaborar el código deontológico de la profesión en cuestión tienen diferentes objetivos, dentro de los cuales se encuentran:

- Llevar a cabo un control independiente y parcial de la actividad profesional.

- Defender los intereses de la profesión.
- Cuidar que la práctica profesional se realice de manera ética y con responsabilidad.
- Ofrecer servicios como bolsa de trabajo o asistencia jurídica cuando sea necesario.
- Establecer sanciones para los profesionales que no cumplan con el código deontológico.
- Asegurar que los profesionales cumplan el código deontológico, y en caso de que se demuestre que algún profesional no lo cumplió se le aplique alguna de las sanciones previamente establecidas. Cualquier persona que considere que un profesional no está cumpliendo con su código deontológico puede denunciarlo con su colegio profesional, sin importar si fue o no el afectado.

El objetivo de los códigos deontológicos es acabar con las malas prácticas en el ámbito profesional, así como brindar satisfacción y seguridad a los clientes, también impulsan el desarrollo de la actividad profesional de forma ética, supervisando y controlando las funciones de los profesionales, con el propósito de que todos los profesionales de una misma área cuenten con una buena imagen.

Después de haber definido lo que es la deontología y los códigos deontológicos, se puede hablar de la deontología dentro del área informática. Como se ha estado mencionando, la tecnología cobra mayor importancia en el día a día, ya que muchas de las actividades cotidianas involucran elementos de TIC, es por ello que surge la deontología informática, ésta involucra todo lo relacionado a los deberes éticos de los profesionales del área de TIC, ya que en sus labores diarias hacen uso de dispositivos tecnológicos y medios de comunicación, y a su vez están en contacto con información confidencial de muchos usuarios, esto quiere decir que los profesionales no son responsables únicamente de aspectos técnicos, sino también de las consecuencias económicas, sociológicas y culturales que trae consigo su profesión, es por ello que deben seguir reglas para garantizar seguridad en la realización de sus labores.

Como todos los profesionales, los del área de informática también cuentan con códigos deontológicos que regulan el uso de los dispositivos que ocupan para realizar sus actividades, así como de la información que almacenan o procesan, ya que deben usar los recursos de TIC de manera profesional, con ética y apegándose a la ley, sin embargo, esto último puede ser un poco complicado, ya que la tecnología al avanzar a pasos agigantados, provoca que las leyes que surjan para regular el uso de las nuevas tecnologías vayan en desfase, en este sentido, los códigos deontológicos sirven de suplemento para dichas leyes.

Asociaciones de profesionales y empresas relacionadas con las TIC han desarrollado códigos deontológicos, los cuales además de guiar la conducta de los profesionales tienen otras funciones, dentro de las cuales se encuentra dar una identidad y estatus profesional a los informáticos como un solo grupo que persigue los mismos objetivos, y ayudar a que la confianza que tiene la sociedad en los profesionales aumente, esto porque permiten que la sociedad sepa cuales son los objetivos del grupo de profesionales.

Como se puede observar, los códigos deontológicos tienen una gran utilidad, por lo que es indispensable que no solo los conozcan y lleven a cabo los profesionales involucrados, sino también es importante que la sociedad sepa de ellos para que colabore concientizándose y de ser posible se hagan las denuncias cuando se detecte que algún profesional no ha respetado su código deontológico.

(Consejo General del Trabajo Social, 2016; Jimenez, 2018; Normativa y Regulación Informática, 2015; Silva & Espina, 2006; Software DELSOL, 2020; Vidal Casero, s. f.)

6.5.3. Contenidos de la ética informática

Como ya se mencionó anteriormente, las tecnologías de la información y comunicación son uno de los campos de estudio de la ética informática, pues regula el uso de los diferentes dispositivos de TIC para que sean usados de tal manera que no se vean afectadas otras personas, adicionalmente, analiza los nuevos problemas, y los que ya existen para determinar en qué medida fueron creados, agravados o transformados por dichas tecnologías, con el objetivo de reconocerlos para posteriormente buscar una solución.

Dentro de los objetivos de la ética informática se encuentran:

- Descubrir los problemas éticos que han surgido gracias a las TIC.
- Proponer principios de actuación para solucionar dichos problemas.
- Regular el uso de las TIC cuando no se tiene alguna ley que regule su uso.
- Evitar daños a otras personas, para de esta forma contribuir con el bienestar de la sociedad.
- Usar las TIC de manera responsable, respetando la privacidad de los demás.
- Acceder a los recursos informáticos con previa autorización.

Asimismo, la ética informática tiene como base los siguientes cuatro principios:

- **Intimidad:** tiene que respetarse la privacidad de la información y no debe compartirse con personas sin autorización, cumpliendo así con el secreto profesional y la confidencialidad.
- **Exactitud:** los responsables de TI deben salvaguardar la información que tienen a su cargo, así como proteger la integridad de la información cuando esta es transmitida.
- **Propiedad intelectual:** se debe respetar la propiedad intelectual y no copiar programas, bases de datos, archivos, entre otros para evitar cometer delitos informáticos.
- **Acceso:** la información tiene que estar disponible únicamente para las personas con autorización.

En 1985 el Brookings Institution, IBM, el Washington Consulting Group y el Washington Theological Consortium fundaron una organización a la cual llamaron Coalition for Computer

Ethics, y en 1992 cambió su nombre a Computer Ethics Institute o CEI (Instituto de Ética Informática) una organización en Estados Unidos, sin fines de lucro que promueve los avances tecnológicos y el uso de las computadoras de forma ética, además, se volvió un grupo que se dedicó la investigación, educación y estudio de políticas. Actualmente, el CEI cuenta con profesionales del área de TIC, organizaciones industriales, grupos académicos y de políticas públicas, quienes trabajan en conjunto para encontrar soluciones a los problemas éticos.

El CEI también es conocido por publicar los 'Diez mandamientos' de la ética informática, estos fueron publicados en un documento que lleva por título "En busca de los 'Diez mandamientos' para la ética informática", el cual fue publicado por Ramón C. Barquín, el objetivo de este documento es guiar a las personas para que usen las TIC de manera ética, es decir, indica a los usuarios el comportamiento que deberían tener para que no perjudiquen a otros usuarios ni su trabajo. Los mandamientos son los siguientes:

1. No usarás una computadora para dañar a otras personas.
2. No interferirás con el trabajo de la computadora de otras personas.
3. No curiosearás en los archivos informáticos de otras personas.
4. No usarás una computadora para robar.
5. No usarás una computadora para dar un falso testimonio.
6. No copiarás ni usarás software propietario por el que no hayas pagado.
7. No utilizarás los recursos informáticos de otras personas sin autorización o compensación adecuada.
8. No deberás apropiarte de la producción intelectual de otras personas.
9. Pensarás en las consecuencias sociales del programa que estás escribiendo o del sistema que estás diseñando.
10. Siempre usarás una computadora de manera que asegure consideración y respeto por los demás.

(Computer Professionals For Social Responsibility, 2011)

Estos mandamientos señalan que no es aceptado dañar a otras personas haciendo uso de una computadora, y que se debe respetar el trabajo y la privacidad de los demás, de igual manera, indica que las computadoras deben usarse de forma ética, por lo que se prohíbe la realización de algún tipo de fraude, así como la obtención de software y recursos de forma ilegal, asimismo, incita a los desarrolladores de software a pensar en los riesgos que podrían tener los usuarios finales con sus desarrollos.

(Encyclopedia.com, s. f.; José, 2022; López Barrientos & Quezada Reyes, 2019)

6.5.4. Actualidad de la ética informática

Las tecnologías de la información y comunicación han sido de gran ayuda, esto debido a que desde algún dispositivo electrónico se puede acceder a diferentes recursos y servicios,

facilitando así las actividades cotidianas de la población en general, además, fueron de gran ayuda durante la pandemia por COVID-19, ya que por ejemplo, los profesores pudieron impartir clases a distancia para que los alumnos las tomaran sin el riesgo de infectarse por COVID-19, asimismo, reuniones laborales pudieron realizarse a distancia usando diferentes medios de videoconferencia, y por otro lado, con el uso de las redes sociales la población en general puede comunicarse con otras personas sin importar su ubicación, pero se dice que este tipo de comunicación ha provocado aislamiento esto porque las personas comenzaron a darle prioridad a su vida virtual, dejando de lado su vida real.

Cabe mencionar que no toda la población tiene acceso a los dispositivos de TI, lo que crea una brecha digital, sin embargo, esto no significa que para el resto de la población la informática no haya tenido un impacto positivo en diferentes aspectos de sus vidas, este impacto no puede medirse con exactitud, ya que la tecnología cambia de manera rápida y constante, pero como se mencionó, la tecnología ha cambiado la forma de realizar las actividades cotidianas en diferentes ámbitos, como el personal, escolar o laboral.

Por otro lado, así como la tecnología ha traído beneficios, también ha traído algunos inconvenientes y dilemas de carácter ético, como el surgimiento de ciberdelitos, donde los delincuentes informáticos usan estas tecnologías para obtener beneficios, realizando actividades ilegales, como el robo de información, violación de derechos de autor, suplantación de identidad y diferentes amenazas más, que comprometen la privacidad de la información almacenada en los sistemas informáticos.

Hoy día, las tecnologías de la información se encuentran presentes en la vida de muchas personas, lo que se vuelve de gran importancia y hace necesario poner atención especial en la ética informática, ya que a través de esta se analizan las consecuencias del uso cotidiano y la alta dependencia que se tiene en la tecnología.

Como me mencionó en el subtema 6.5.1, la ética informática se encarga de analizar los problemas que son generados, agravados o transformados por la tecnología, del mismo modo, la ética informática permite demostrar la capacidad ética y moral de los usuarios de las tecnologías.

Debido a que el desarrollo de las tecnologías ha tenido gran importancia y ha generado muchos cambios en la humanidad, las escuelas que cuentan con carreras relacionadas con las TIC se han tenido la necesidad de incluir en sus planes curriculares la ética informática, esto con la finalidad de hacer conscientes a los futuros profesionales de que las acciones que lleven a cabo haciendo uso de los dispositivos informáticos van a repercutir en los demás, por lo que la ética informática ayudará a determinar lo que es correcto y lo que no en la sociedad, aunque lo que es correcto en una sociedad no significa que sea correcto en otra.

La ética informática sigue buscando que las y los profesionistas ejerzan sus actividades profesionales con responsabilidad y respeto, siempre buscando un bienestar individual y

colectivo, además busca guiar las acciones de los profesionales y usuarios en general ante determinadas situaciones, para que puedan decidir de manera individual qué es lo que se considera como bueno y como malo para que actúen dependiendo de los criterios establecidos.

Aunque por la brecha digital existente, es posible que muchos de los usuarios no sean conscientes de la existencia de la ética informática, sin embargo, en este punto la moral tiene un papel importante, ya que ésta le indica a cada persona de manera individual si determinadas acciones son buenas o malas, por lo que sin conocer la ética informática podría actuar con base en sus principios morales para determinar si alguna acción es considerada como buena o mala, y cómo la toma de ciertas acciones podría influenciar en su entorno.

Ante la falta de conocimiento sobre la ética informática, se puede observar que es importante concientizar a los usuarios menos familiarizados con el tema, orientarlos para que hagan uso de la tecnología con mayor seguridad y concientizarlos sobre la existencia y usos que tiene la ética informática.

Si bien es cierto, siempre habrá ciberdelincuentes buscando víctimas de las cuales puedan obtener algún tipo de beneficio, buscando y explotando las vulnerabilidades que estén a su alcance, asimismo, podría verse una reducción en la cantidad de víctimas si los usuarios son conscientes del riesgo que corren al compartir información personal en sitios no seguros, además al impulsar el uso de la ética informática en el día a día los usuarios sabrían que algunas de las acciones que realizan pueden directa o indirectamente afectar a otros.

Por otro lado, instruir a los profesionales del área de tecnología acerca de la ética informática debería ser considerado una prioridad, porque podría darse el caso que no tengan el conocimiento suficiente sobre lo que implica trabajar siguiendo lo establecido por la ética informática, asimismo, es importante que las escuelas se preocupen por la impartición de materias que ayuden a los estudiantes a irse familiarizando con este tipo de temas, que son de vital importancia dentro del área.

(SNK, 2018; Sosa Barrientos et al., 2015; Triana Tacuma, 2017)

6.5.5. Psicología del intruso

De acuerdo con la Asociación Americana de Psicología, la psicología es la ciencia que estudia y analiza los procesos mentales del ser humano, para comprender cómo estos afectan su comportamiento y la interacción que tiene con su entorno físico y social, responde a preguntas como “¿Por qué el ser humano actúa de cierta manera?” o “¿Qué factores influyen en su personalidad y desenvolvimiento social?”.

La información que se recolecta sobre la conducta humana es organizada de manera sistemática, para posteriormente elaborar teorías para su comprensión, haciendo esto se puede explicar el comportamiento humano e incluso predecir sus acciones futuras.

Dentro de la psicología hay un área llamada psicología criminológica, esta área estudia los procesos mentales y el comportamiento involucrado en los delitos. Los delitos llevados a cabo dentro del área de la informática son conocidos como ciberdelitos o delitos informáticos, y actualmente por la importancia de la tecnología en la vida cotidiana son considerados una de las amenazas más graves en el mundo.

La ingeniería social (tema 3.2.5) usa principalmente psicología, ya que, al aplicarla, el atacante busca manipular a la víctima, para comprender cómo es su forma de pensar y saber de qué manera puede influenciar en ella, para así obtener una respuesta que le sea útil y le brinde información que le ayude a obtener mayores beneficios.

Las organizaciones podrían tener implementados los mejores sistemas de seguridad para proteger sus activos, sin embargo, como se mencionó en el tema 3.2.5, el ciberdelincuente al usar ingeniería social intenta conseguir la confianza la víctima para después aprovecharse de eso y acercarse más a su objetivo, por lo que si el atacante consigue manipular a las víctimas serviría de poco que la organización tenga los mejores sistemas de seguridad implementados si mediante manipulación el atacante obtendrá acceso a sistemas o información que sea de su interés.

Hay diferentes tipos de ciberdelitos, los cuales le permiten a un delincuente cibernético no solo atacar a las grandes empresas, sino también a empresas pequeñas, medianas e incluso a usuarios, que dependiendo del tipo de información que posean y las características particulares de su participación en la sociedad le indicarán al delincuente el tipo de ataque que debiera realizar y que pone en gran riesgo a quienes posean dicha información creyendo que esta no es valiosa o que no puede ser de utilidad para algún atacante.

Muchas veces la falta de conciencia en temas de seguridad informática o la creencia de que no tienen información importante en la cual un atacante pueda estar interesado es lo que hace que las empresas, personas u organizaciones bajen la guardia, volviéndose más vulnerables y haciendo que las probabilidades de éxito del atacante aumenten considerablemente. Por ejemplo, los atacantes pueden usar ransomware para aprovecharse del miedo de la víctima a perder información importante, también pueden usar ingeniería social para conseguir que la víctima confíe en ellos y les brinden información útil, e incluso a través llamadas telefónicas, mensajes de texto o correos electrónicos pueden hacerse pasar por algún familiar, amigo, conocido e incluso operador del banco de la víctima para obtener información o algún beneficio económico.

¿Qué es lo que impulsa a un ciberdelincuente a realizar los delitos informáticos? Hay muchos motivadores, entre ellos los beneficios económicos, diversión o simplemente poner a prueba

sus propias habilidades e inteligencia, en el tema 2.1, dentro de las fuentes de amenaza humanas se mencionan los diferentes tipos de hackers, los cuales se clasifican de acuerdo al motivo por el que penetran en los sistemas, por lo que los tipos de hackers se dividen en:

- **White hat:** también son conocidos como hackers éticos, estos penetran en los sistemas teniendo previa autorización, con el objetivo de encontrar vulnerabilidades para posteriormente reportarlas a los responsables para que sean reparadas. Los hackers éticos son los que ayudan a las organizaciones a mantener sus sistemas seguros, pues, se comprometen a no revelar las vulnerabilidades encontradas.
- **Black hat:** este tipo de hackers, al contrario de los white hat, penetran en los sistemas sin tener autorización, lo hacen con el propósito de perjudicar a las víctimas y conseguir información que puedan usar en su beneficio. Los hackers black hat no se rigen por algún código ético, por lo que para ellos no es importante respetar las leyes, sino, obtener un beneficio propio.
- **Gray hat:** este tipo de hackers penetran en los sistemas sin tener previa autorización para descubrir sus vulnerabilidades, por lo que sus acciones siguen siendo ilegales, a diferencia de los black hat, los gray hat no se aprovechan de las vulnerabilidades que encuentran, sin embargo, es posible que publiquen sus hallazgos en internet, por lo que otros hackers podrían explotar las vulnerabilidades para obtener un beneficio. Una práctica conocida, por ejemplo, es que después de encontrar las vulnerabilidades del sistema de la organización se comunican con esta y le ofrecen sus servicios o los de uno de sus colegas para corregirlos.

No cabe duda que los delincuentes cibernéticos y los hackers éticos son grandes conocedores en informática, que entienden muy bien cómo usar los sistemas y dispositivos de TIC en su beneficio, sin embargo, el propósito con el que aplican sus conocimientos es lo que hace la diferencia, ya que un hacker ético buscará beneficiar a la empresa u organización, descubriendo fallas en sus sistemas para prevenir que un delincuente informático se aproveche de dichos fallos y vulnerabilidades para perjudicar a las víctimas.

Los usuarios necesitan mucho más que solo comprender la forma de pensar de los delincuentes informáticos, necesitan estar conscientes de los riesgos que conlleva la interacción con los dispositivos de TIC e internet para usarlos de forma segura, para reducir los riesgos a los que se exponen.

(Centro de Estudios y Servicios en Salud, s. f.; Hofmann, 2021; J. Jiménez, 2022; Martínez Alarcón, 2006; Maza Correa, 2023; Molinetti, 2020; Panda Security, 2023)

6.5.6. Códigos de ética

Un código de ética es un documento que contiene principios y valores que regulan el comportamiento de un grupo de personas, estos se apoyan en la deontología, ya que como se menciona en el subtema 6.5.2, la deontología guía la conducta profesional.

Puede decirse que la existencia de los códigos de ética se remonta al siglo XVIII a.C con el código de Hammurabi, si bien este código no fue la primera ley escrita sí se encuentra entre las primeras leyes de la historia, éste fue importante porqué influyó en la creación de las leyes de otras culturas, dicho código fue promulgado por el rey Hammurabi de babilonia y consta de 282 leyes, que regulaban entre otras cosas los contratos de negocios y precios de los productos, cada una de las leyes tenía un castigo que debía ser afrontado por quienes no cumplieran la ley, entre estos castigos se encontraba la pena de muerte y la ley de Talión, expresada como ”ojo por ojo y diente por diente”, la cual indica que el infractor de la ley debe recibir un castigo que le provoque un daño como el que causó.

Los códigos de ética pueden ser elaborados por una organización para regular el comportamiento de todos los profesionales del área, asimismo, las empresas pueden elaborar sus propios códigos de ética apegados a su cultura organizacional para que sean llevados a cabo por todos sus integrantes, destacando su misión, visión y valores.

El incumplimiento de alguno de los principios de los códigos de ética no implica alguna sanción legal, sin embargo, esto no significa que no sea obligatorio cumplirlos, ya que, al regular el comportamiento de un grupo de personas, en este caso de profesionales, la sociedad puede confiar en que desarrollarán sus actividades de manera ética, lo cual es importante para que una profesión cuente con una buena imagen, reduciendo los conflictos y protegiendo la reputación de los profesionales o de los integrantes de la empresa.

El propósito de los códigos de ética, como ya se mencionó es guiar la conducta de un grupo de personas, además de establecer un conjunto de valores que deberán ser respetados por el grupo de profesionales o en dado caso por los integrantes de una empresa, además pueden servir de guía para tomar decisiones, teniendo en cuenta los intereses internos y externos de las empresas.

Si bien cada código de ética es elaborado para cumplir con las necesidades específicas de una empresa u organización, hay algunos criterios que de manera común pueden encontrarse en diferentes códigos de ética, por ejemplo: no divulgar información confidencial y dar un trato igualitario a clientes y compañeros de trabajo sin importar su nacionalidad, cultura o religión, es decir, los códigos de ética ayudan a generar confianza y a resolver conflictos dentro y fuera de la empresa u organización, manteniendo una buena imagen y credibilidad.

Los códigos de ética ayudan entre otras cosas a:

- Concientizar a los miembros de la importancia que tiene que los valores profesionales sean respetados y cumplidos.
- Promover un comportamiento ético, profesional y respetuoso entre los miembros, clientes y proveedores de las empresas y organizaciones, evitando todo tipo de discriminación.
- Hacer que todos los miembros de la organización o empresa sean conscientes de la responsabilidad social que tienen en su comunidad.
- Favorecer un buen ambiente laboral y crear una sensación de seguridad en todos los involucrados.
- Orientar a todos los integrantes para que actúen con imparcialidad en las diferentes situaciones.
- Prevenir situaciones de riesgo que afecten su reputación, credibilidad e imagen.

Tomando en cuenta todo lo anterior, los códigos de ética ofrecen grandes beneficios, esto porque todas las decisiones que se tomen en el ámbito profesional afectan de una u otra forma a la organización o empresa, por lo que un código de ética ayudará a implementar buenas prácticas e incluso le permitirá a las empresas y organizaciones mejorar su imagen lo cual es fundamental para tener éxito dentro del área.

Donald Gotterbarn fue uno de los pioneros en reconocer y promover la importancia de la ética entre los profesionales del área de la informática y junto a un equipo de trabajo participó en la creación de los códigos de ética del IEEE (Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos) y la ACM (Association for Computing Machinery o Asociación de Maquinaria Computacional), de los cuales se hablará a continuación por su amplio reconocimiento a nivel mundial.

(Comisión de Derechos Humanos del Estado de México, s. f.; Hernández, 2021; Sosa Barrientos et al., 2015; Universidad de los Andes, s. f.; Vidal Casero, s. f.)

6.5.6.1. ACM Code of Ethics and Professional Conduct

La ACM cuyas siglas derivan del inglés Association for Computing Machinery o en español conocida como Asociación de Maquinaria Computacional, es una organización fundada en 1947, reconocida como la primera sociedad científica y educativa sobre las ciencias de la computación y ciencias afines, en la actualidad cuenta con más de 92,000 miembros a nivel mundial y es la asociación número uno para los profesionales en computación.

El código de ética y conducta profesional de la ACM se conforma de un preámbulo y cuatro secciones:

- **Preámbulo:** se menciona que la informática es un área donde las decisiones que tomen los profesionales deben hacerse de manera responsable, adicionalmente, menciona que

el propósito de este código es guiar la conducta de todos aquellos que utilicen la informática para generar impacto, entre ellos los estudiantes, profesionales actuales, futuros e instructores.

1. **Sección 1. Principios éticos generales:** en esta sección se describen los siete principios fundamentales del código.
   Un profesional de la informática debería:
   - **1.1.** Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la informática.
   - **1.2.** Evitar el daño.
   - **1.3.** Ser honesto y confiable.
   - **1.4.** Ser justo y tomar medidas para no discriminar.
   - **1.5.** Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos.
   - **1.6.** Respetar la privacidad.
   - **1.7.** Respetar la confidencialidad.

2. **Sección 2. Responsabilidades profesionales:** indica las responsabilidades específicas de los profesionales.
   Un profesional de la informática debería:
   - **2.1.** Esforzarse por lograr una alta calidad tanto en los procesos como en los productos del trabajo profesional.
   - **2.2.** Mantener altos estándares de competencia profesional, conducta y práctica ética.
   - **2.3.** Conocer y respetar las reglas vigentes relacionadas con el trabajo profesional.
   - **2.4.** Aceptar y proporcionar una revisión profesional adecuada.
   - **2.5.** Realizar evaluaciones integrales y exhaustivas de los sistemas informáticos y de sus impactos, incluyendo un análisis de los posibles riesgos.
   - **2.6.** Trabajar solo en sus ámbitos de competencia.
   - **2.7.** Fomentar la conciencia ciudadana sobre la informática, las tecnologías relacionadas y sus consecuencias.
   - **2.8.** Acceder a los recursos informáticos y de comunicación solo cuando esté autorizado, o cuando sea necesario para proteger el bien público.
   - **2.9.** Diseñar e implementar sistemas robustos accesibles y seguros.

3. **Sección 3. Principios de liderazgo profesional:** esta sección hace referencia a que los lideres tienen una mayor responsabilidad de promover y defender los principios.
   Un profesional de la informática, especialmente quien cumpla funciones de liderazgo, debería:
   - **3.1.** Asegurar que el bien público sea la preocupación central en el trabajo profesional.

3.2. Articular, fomentar la aceptación y evaluar el cumplimiento de las responsabilidades sociales por parte de los miembros de la organización o grupo.
3.3. Administrar el personal y los recursos para mejorar la calidad de la vida profesional.
3.4. Articular, aplicar y apoyar políticas y procesos que reflejen los principios del código.
3.5. Crear oportunidades para que los miembros de la organización o el grupo crezcan como profesionales.
3.6. Tener cuidado al modificar o retirar sistemas.
3.7. Reconocer y cuidar los sistemas que se integran en la infraestructura de la sociedad.

4. **Sección 4. Cumplimiento del código:** esta última sección se refiere a que los principios del código deben ser cumplidos y promovidos, así como que los miembros de la ACM deben reconocer cuando alguno de los principios sea violado y reportarlo con la ACM. Un profesional de la informática debería:
   4.1. Defender, promover y respetar los principios del código.
   4.2. Tratar las violaciones del código como inconsistentes con la afiliación a ACM.

(ACM, s. f.)

6.5.6.2. Institute of Electric and Electronic Engineers

La IEEE que deriva del inglés Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos por su significado en español es una organización que surgió después de fusionar dos organizaciones, la AIEE (American Institute of Electrical Engineers o Instituto Americano de Ingenieros Eléctricos), fundada en 1884 por Thomas A. Edison y Alexander G. Bell y el IRE (Institute of Radio Engineers o Instituto de Ingenieros de Radio), fundada en 1912, estas dos organizaciones se fusionaron y el 1 de enero de 1963 es como nace la IEEE, ésta es una organización que contribuye con un 30% de la información técnica de los avances tecnológicos a nivel mundial, y tiene como propósito fomentar la innovación tecnológica para el beneficio de la humanidad.

(IEEE Sección España, s. f.)

La IEEE reconoce la importancia de la tecnología en la humanidad, por lo que redactó su propio código de ética, el cual se encuentra escrito en forma de decálogo y se muestra a continuación:

- Aceptar la responsabilidad de tomar decisiones que favorezcan el bienestar de las personas, así como poner en evidencia cualquier factor que pueda tener impactos negativos en las personas o el medio ambiente.
- Evitar los conflictos de interés y revelarlos en caso de que existan.
- Ser realistas y honestos al realizar afirmaciones y estimaciones.
- Rechazar los sobornos.

- Desarrollar el conocimiento de la tecnología, así como sus aplicaciones y analizar las posibles consecuencias.
- Mantener e incrementar las competencias técnicas y asumir tareas tecnológicas para otras personas sólo cuando se está facultado para ello.
- Buscar, ofrecer y aceptar críticas justas sobre el trabajo, reconociendo los errores y dando crédito a las contribuciones realizadas por otras personas.
- Tratar de forma equitativa a todas las personas, sin incurrir en acciones discriminatorias.
- Evitar el daño a la reputación, el empleo o la propiedad de otros, mediante falsedades o acciones malintencionadas.
- Ayudar a que los compañeros de trabajo y colegas se desarrollen profesionalmente, así como a que cumplan también las normas de este código ético.

Como se puede observar, este código de ética también promueve que los profesionales tengan conductas éticas, para aportar positivamente en la sociedad.

(Filgueiras Nodar, 2017)

6.5.6.3. Código de ética y ejercicio profesional de ingeniería de software

Este código de ética fue dirigido por Donald Gotterrbarn y aprobado por la ACM y la IEEE, y está dirigido principalmente para los profesionales del área de ingeniería de software, debido a lo importante que es el software en la vida cotidiana, por lo que también es muy importante regular su creación.

La versión 5.2 de este código de ética se conforma de un preámbulo y ocho principios.

- **Preámbulo:** reconoce la importancia de las computadoras para las actividades cotidianas, ya sea para entretenimiento, educación, negocios, entre otros usos, y que los ingenieros de software tienen un papel importante en el análisis, diseño, desarrollo, mantenimiento y prueba de dichos sistemas, por lo que es importante que los ingenieros de software realicen su trabajo teniendo como base este código de ética, el cual les permitirá distinguir las acciones éticas de las que no lo son.

La versión resumida de los ocho principios es la siguiente:

Los ingenieros de software deberán:

1. **Público:** actuar consistentemente con el interés público.
2. **Cliente y empleador:** actuar de una forma determinada que esté en los mejores intereses de su cliente y empleador consistente con el interés público.

3. **Producto:** asegurar que sus productos y modificaciones relacionadas logren el más alto estándar profesional posible.
4. **Juicio:** mantener integridad e independencia al emitir su juicio profesional.
5. **Gerencia:** los gerentes y líderes de ingeniería de software deberán suscribirse y promocionar un enfoque ético para la gerencia de desarrollo y mantenimiento de software.
6. **Profesión:** fomentar la integridad y reputación de la profesión consistente con el interés público.
7. **Colegas:** ser justos y comprensivos con sus colegas.
8. **Interés propio:** participar en el aprendizaje de por vida del ejercicio de su profesión y deberán promover un enfoque ético para el ejercicio de la misma.

(Código de Ética y ejercicio profesional de ingeniería de software. Versión 5.2)

6.6. Impacto social de la seguridad informática

Como consecuencia de la pandemia por COVID 19 aumentó considerablemente el uso de las TIC. En la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2021, elaborada por el Instituto Nacional de Estadística y Geografía o INEGI se muestra que en 2021 en México:

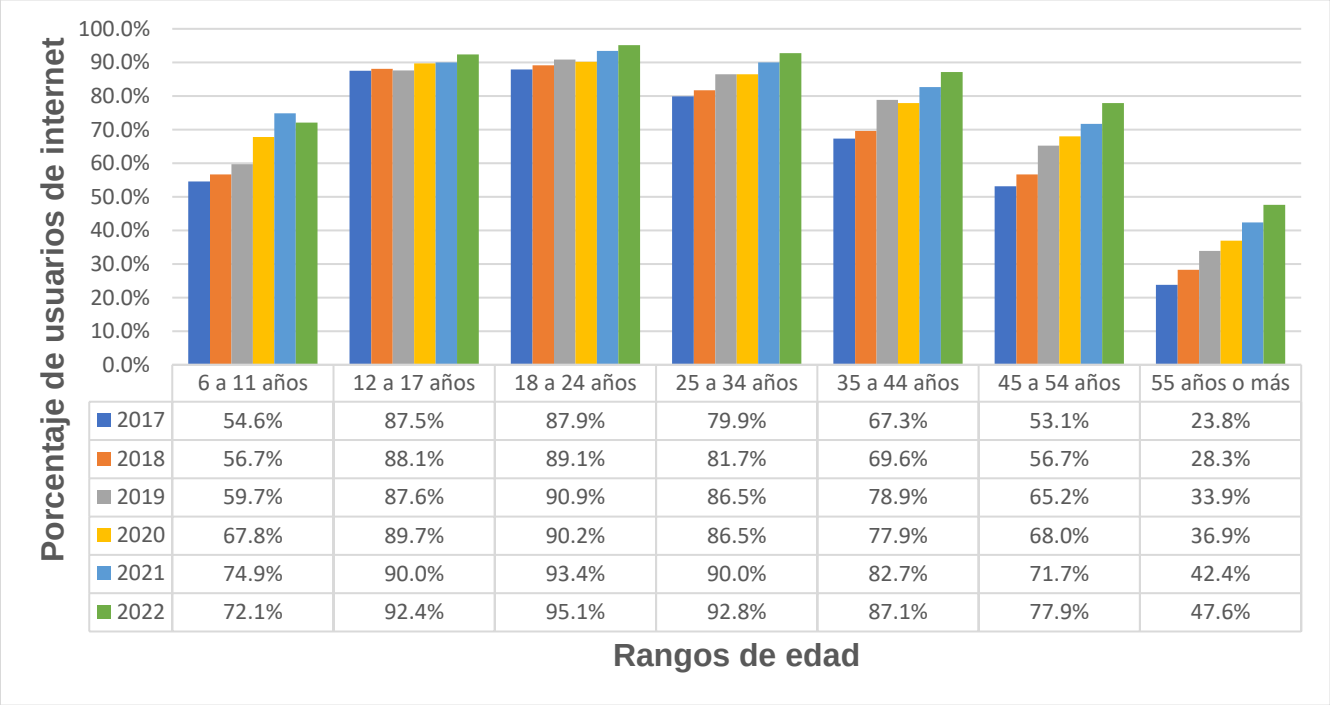
- El 75.6% de la población mayor a seis años es usuaria de internet.
- El 78.3% de la población cuenta con un teléfono celular.
- El 37.4% de la población mayor a seis años es usuaria de computadoras.

Comparando estos datos con la encuesta realizada en el año 2022, se tiene lo siguiente:

- El 78.6% de la población mayor a seis años es usuaria de internet.
- El 79.2% de la población cuenta con un teléfono celular.
- El 37% de la población mayor a seis años es usuaria de computadoras.

Estos datos muestran cómo en un año el uso de las tecnologías cambia, se puede observar claramente que el número de usuarios de internet va en aumento, ya que en un año la cantidad de usuarios incrementó en un 3%, lo que de acuerdo con los estudios significa que el número de usuarios subió en un orden de 4.5 millones de usuarios en un año, contando en 2021 con 88.6 millones de usuarios, mientras que en 2022 fueron 93.1 millones.

En la figura 6.1 se observa el porcentaje de usuarios de internet por grupo de edad:



	6 a 11 años	12 a 17 años	18 a 24 años	25 a 34 años	35 a 44 años	45 a 54 años	55 años o más
2017	54.6%	87.5%	87.9%	79.9%	67.3%	53.1%	23.8%
2018	56.7%	88.1%	89.1%	81.7%	69.6%	56.7%	28.3%
2019	59.7%	87.6%	90.9%	86.5%	78.9%	65.2%	33.9%
2020	67.8%	89.7%	90.2%	86.5%	77.9%	68.0%	36.9%
2021	74.9%	90.0%	93.4%	90.0%	82.7%	71.7%	42.4%
2022	72.1%	92.4%	95.1%	92.8%	87.1%	77.9%	47.6%

Figura 6.1. Población usuaria de internet en México.

En la figura anterior se puede observar que el número de usuarios de internet aumenta cada año, siendo los rangos de 12 a 17 y de 18 a 24 años donde se concentra la mayor cantidad de usuarios, mientras que el rango de 55 años o más es el grupo que cuenta con una menor cantidad de usuarios de internet.

Algo interesante a tomar en cuenta es que en el año 2020 incrementó el número de usuarios entre 6 y 11 años en un 8.1% el cual es considerable respecto a años anteriores, esto podría deberse a que fue en este año cuando debido a la pandemia por COVID-19 se comenzaron a realizar las actividades en línea, asimismo, se puede observar que hubo un decremento en usuarios de este rango de edad en 2022 disminuyendo en un 2.8%, esto podría ser debido a que en este año se comenzaron a retomar las actividades presenciales en las escuelas, por lo cual podría darse esta disminución.

En dicha encuesta también se menciona que la mayor cantidad de usuarios que acceden a internet lo hacen usando un teléfono inteligente, mientras que el porcentaje de usuarios que acceden a través de una computadora portátil, tableta electrónica o computadora de escritorio mostró una disminución a partir del año 2019.

En la figura 6.2 se observan los principales usos de internet de los años 2021 y 2022:

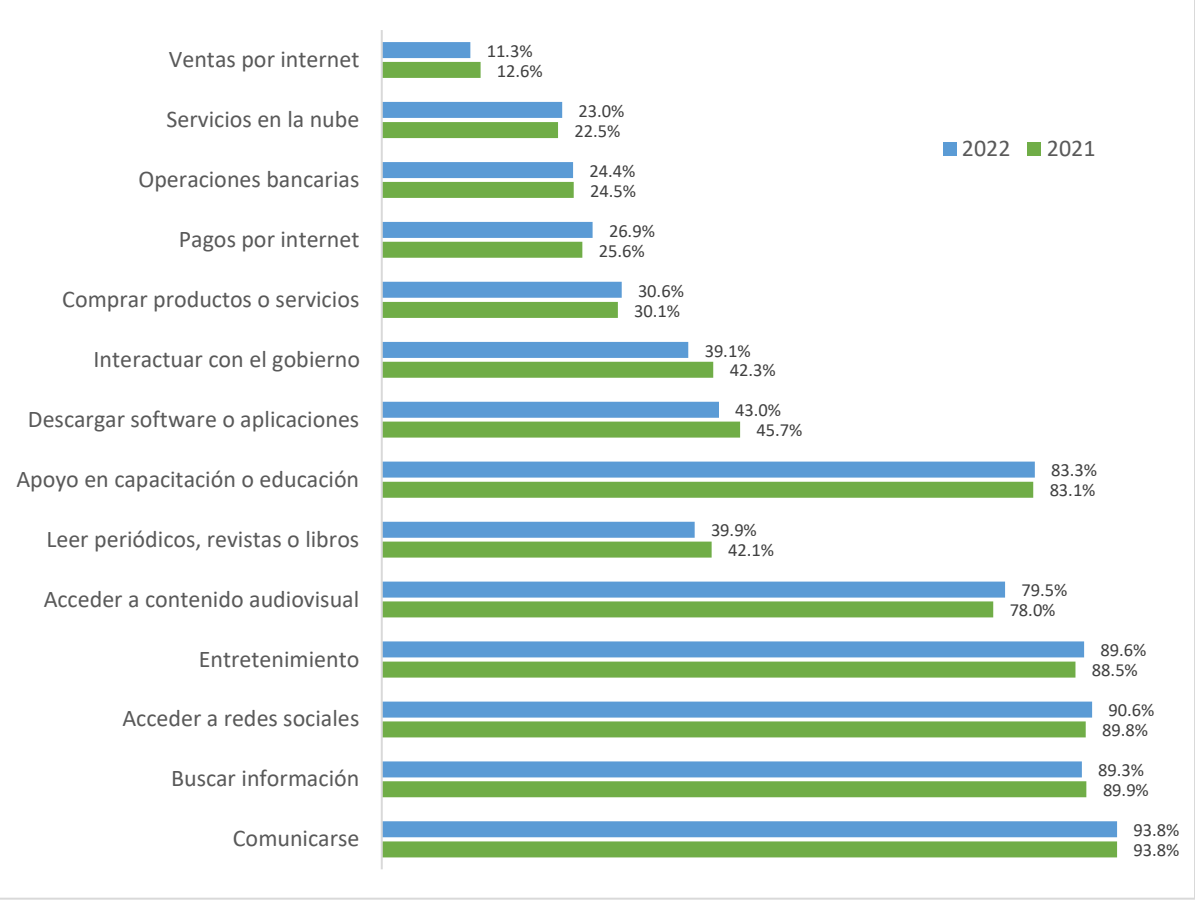


Figura 6.2. Principales usos de internet.

De acuerdo con el gráfico anterior, los mayores usos que le dieron los usuarios a internet en 2021 y 2022 es el siguiente:

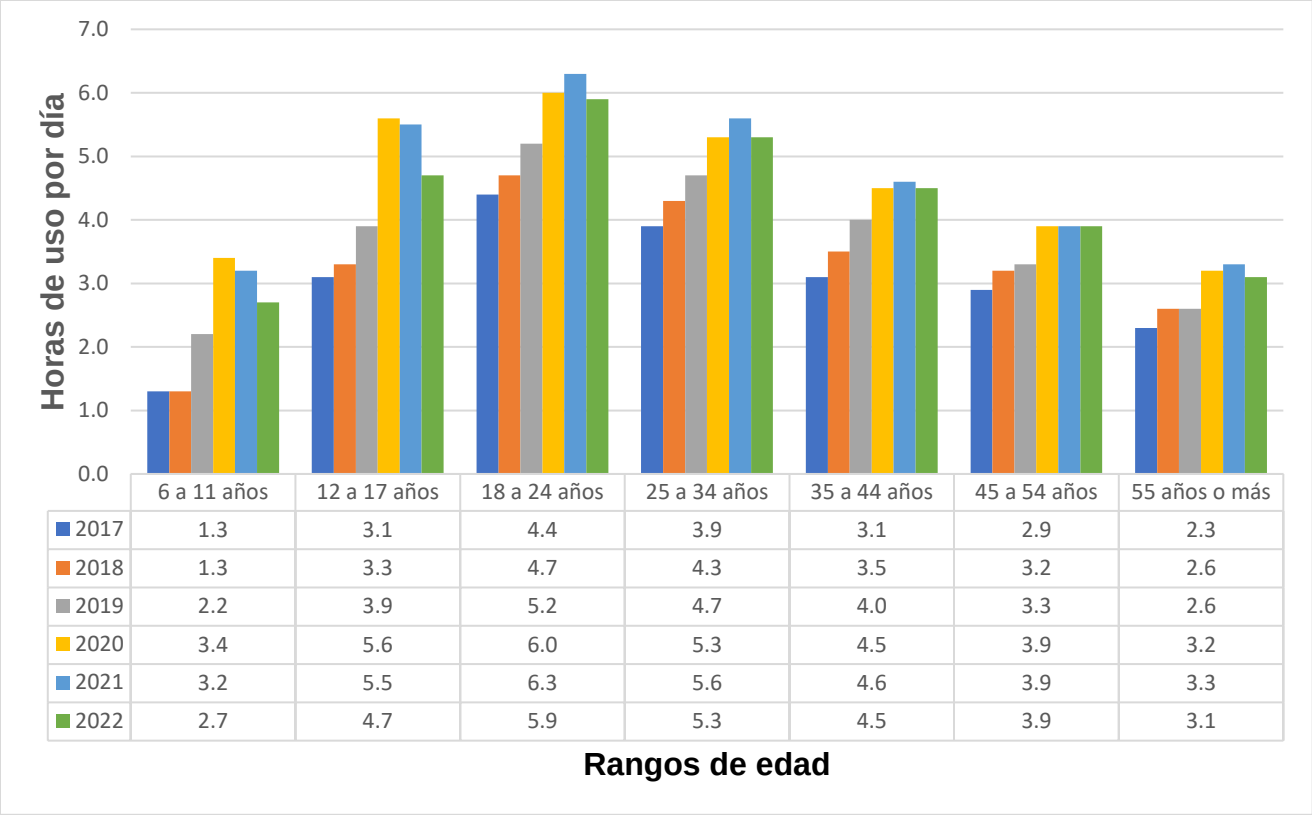
Mayores usos	2021	2022
Comunicarse	93.8%	93.8% –
Buscar información	89.9%	89.3% ▼
Acceder a redes sociales	89.8%	90.6% ▲
Entretenimiento	88.5%	89.6% ▲
Apoyo en capacitación o educación	83.1%	83.3% ▲
Acceder a contenido audiovisual	78%	79.5% ▲

Tabla 6.2. Mayores usos de internet 2021 y 2022

Cabe mencionar que los porcentajes del año 2021 podrían estar estrechamente relacionados con la pandemia por COVID 19, ya que, muchas de las actividades que se hacían de forma presencial cambiaron a una modalidad en línea, por ende, hubo muchas personas que comenzaron a comunicarse más por medio del internet, del mismo modo, muchas escuelas comenzaron a impartir clases en línea, por lo que la búsqueda de información en internet tuvo un aumento, haciendo que para el año 2021 se posicionara como la segunda actividad más realizada usando internet.

Respecto al año 2022, el mayor uso que le dieron los usuarios a internet fue para comunicarse, esta puede llevarse a cabo por medio de las diferentes aplicaciones de mensajería, lo que tiene sentido si se toma en cuenta que en el año 2022 el segundo mayor uso que los usuarios le dieron a internet fue el acceso a redes sociales. Adicionalmente, se puede observar una ligera disminución en el apoyo en capacitación o educación, lo cual es un reflejo de que fue en este año cuando las actividades presenciales se retomaron.

También se muestra en la figura 6.3 la cantidad de horas promedio que cada uno de los rangos de edad pasa en internet al día.



	6 a 11 años	12 a 17 años	18 a 24 años	25 a 34 años	35 a 44 años	45 a 54 años	55 años o más
2017	1.3	3.1	4.4	3.9	3.1	2.9	2.3
2018	1.3	3.3	4.7	4.3	3.5	3.2	2.6
2019	2.2	3.9	5.2	4.7	4.0	3.3	2.6
2020	3.4	5.6	6.0	5.3	4.5	3.9	3.2
2021	3.2	5.5	6.3	5.6	4.6	3.9	3.3
2022	2.7	4.7	5.9	5.3	4.5	3.9	3.1

Figura 6.3. Uso de internet promedio por día.

Algo interesante de notar en la figura 6.3 es que las horas de uso del internet al día tuvieron un aumento considerable en el año 2020 en todos los grupos de edad, esto coindice con el inicio de la pandemia por COVID 19, esto podría deberse a que muchas de las actividades que solían hacerse de manera presencial comenzaron a realizarse en línea, esto como una medida de prevención para evitar un aumento en el número de casos por dicha enfermedad.

En el contexto internacional, el uso de internet por parte de los países mostrados en la encuesta se observa en la figura 6.4:

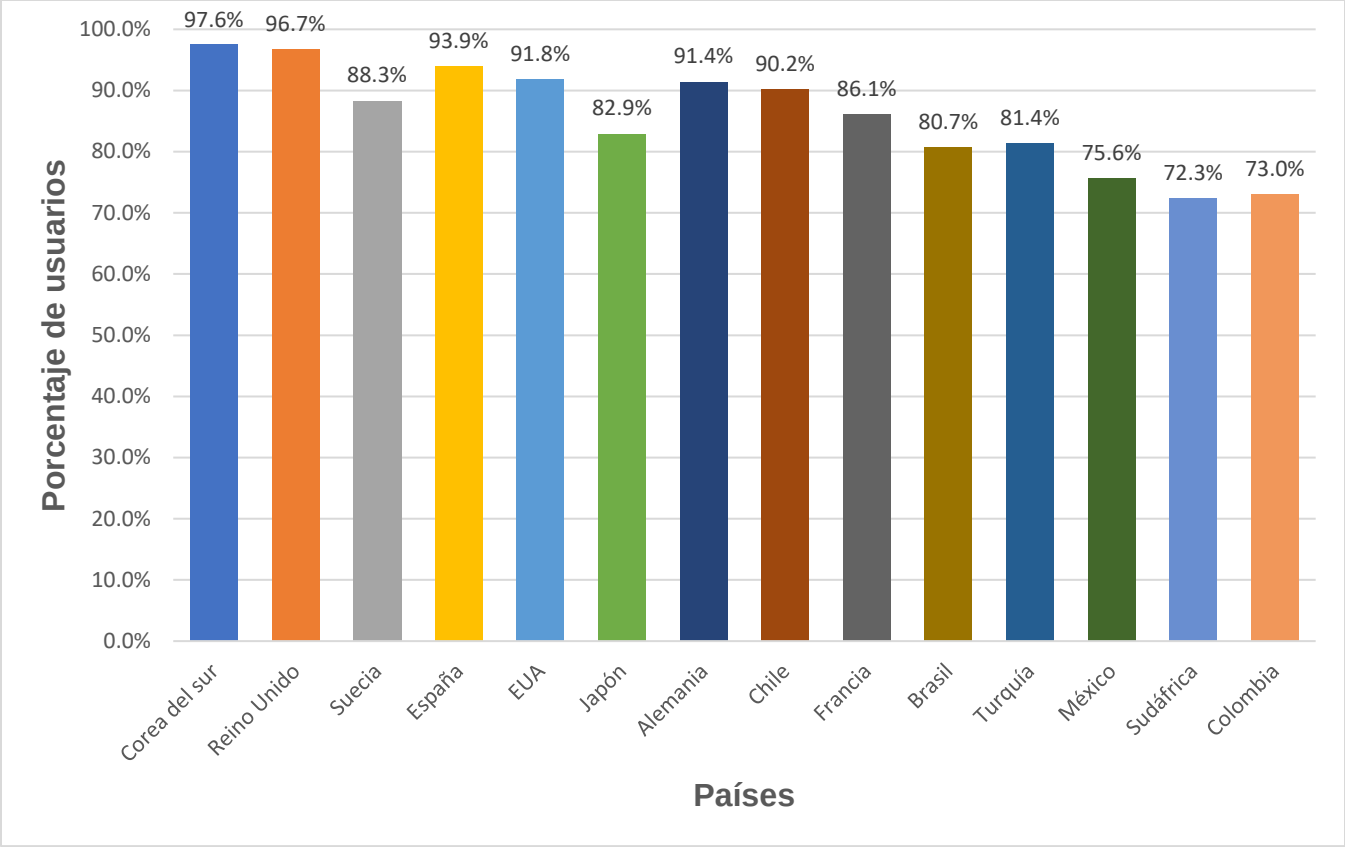


Figura 6.4. Uso de internet internacionalmente.

De acuerdo con datos de la encuesta realizada en 2021 se puede observar que Corea del sur es el país que cuenta con una mayor cantidad de usuarios de internet (97.6%), seguido de Reino Unido (96.7%), en tercer lugar, se encuentra España (93.9%), en cuarto lugar, Alemania (91.4%) y en quinto lugar USA (91.8%).

(INEGI & IFT, 2022, 2023)

Teniendo en cuenta la información proporcionada anteriormente se tiene un panorama más amplio del uso de internet, que como se observa actualmente, se usa en la mayoría de las actividades cotidianas, desde la comunicación, hasta el entretenimiento, por lo que puede entenderse que la ciberseguridad es indispensable para proteger toda la información que circula por internet diariamente.

El uso de las TIC ha facilitado la vida de los usuarios de manera importante, puesto que es mucho más fácil la forma de comunicarse y/o acceder a información, sin embargo, esto ha traído consigo muchos riesgos y amenazas a la seguridad, los cuales aumentan con el paso del tiempo, por lo que para usar las TIC de manera segura se debe tener conocimiento de las situaciones de riesgo que podrían poner en peligro la información de los usuarios, de igual manera, quienes navegan en internet por cuenta propia deben estar conscientes del tipo de información que comparten, en dónde la comparten y con quién lo hacen, ya que muchos de

los usuarios no están conscientes de los riesgos a los que se exponen al usar las TIC sin las medidas de seguridad apropiadas.

Los usuarios de las TIC como gobiernos, organizaciones, instituciones o particulares se vuelven propensos a ser víctimas de ataques desde el primer momento que se conectan a la red o comparten información sin importar el dispositivo que utilicen y debido a la importancia que tiene el uso de las TIC en la realización de actividades cotidianas, los ataques cibernéticos son muy comunes.

La seguridad informática es de suma importancia tomando en cuenta el mundo digitalizado en el que vivimos actualmente, por lo que la ciberseguridad va a ser útil para aumentar la seguridad en organizaciones, gobiernos o usuarios de diferentes servicios.

Muchas de las personas que hacen uso de las TIC no son conscientes de los riesgos que pueden correr al realizar diferentes acciones en internet o quizá piensen que su información no es tan importante como para ser objetivo de algún ataque, sin embargo, no hay que olvidar que la información es el activo más importante por lo que no hay que descuidar su seguridad. Por ejemplo, muchos de los usuarios de redes sociales comparten información detallada, como fechas de cumpleaños, nombres de familiares o mascotas, lugar de trabajo e incluso el lugar donde viven, con este tipo de información, podrían ser víctimas de suplantación de identidad, extorsión o en casos extremos podrían ser víctimas de situaciones donde se vean afectados físicamente, como robos o secuestros, esto significa que hay que saber qué tipo de información se puede compartir sin que llegue a representar un peligro.

Como se mencionó en la encuesta realizada por el INEGI, la mayoría de los usuarios de internet acceden a esta red por medio de sus teléfonos celulares, por lo que es importante protegerlos ya que en estos dispositivos se almacena una gran cantidad de información y se puede acceder a muchos sitios diferentes, como a cuentas de banco por medio de la banca móvil, redes sociales o correo electrónico, igualmente se pueden realizar muchas actividades, entre ellas llamadas telefónicas, videollamadas, o envío de mensajes a través de aplicaciones como whatsapp, telegram, messenger, entre otras, por ello es importante que el acceso a este tipo de dispositivos esté protegido, para ello se puede hacer uso de contraseñas, patrones de bloqueo o sensores biométricos. Como se puede observar todo aquel dispositivo que tenga una conexión al mundo de internet requiere contar con contraseñas de seguridad para acceder, así como el uso de antivirus o antimalware.

El acceso a servicios en internet también debe tener un buen nivel de seguridad, contar con contraseñas con las características descritas en el tema 3.2.1, así como verificar que los sitios donde se comparte información sean seguros y legítimos.

Por otro lado, las organizaciones deben tener mucho cuidado manejando la información personal de sus clientes, así como la información que la organización maneja de manera interna y que podría resultar de gran interés para los atacantes.

Se podría pensar que las grandes organizaciones y los gobiernos son los únicos que podrían ser víctimas de ataques, sin embargo, las pequeñas y medianas organizaciones no están exentas ya que como se ha mencionado con anterioridad, los atacantes buscarán cualquier tipo de información que les proporcione algún beneficio.

Las organizaciones deben considerar la aplicación de medidas de seguridad como una inversión y no como un gasto, esto porque al mantener sus sistemas e información protegidos podrán brindar confianza a sus clientes y a su vez les será útil para mantener una buena reputación dentro del mercado, es por ello que deben invertir en la protección de sus sistemas informáticos, ya que es ahí donde se almacena la información que ayuda a aumentar su productividad.

La seguridad informática dentro de los gobiernos también tiene un papel muy importante actualmente, ya que, si esta información que almacenan es vulnerada, la seguridad de todo el país y sus ciudadanos se ve comprometida.

Hay que recordar que la seguridad informática no solo se refiere a proteger de información o datos almacenados de manera electrónica, de igual manera se incluye la protección de los sistemas y dispositivos que almacenan información, así como la protección de la infraestructura de las organizaciones y a los empleados. Asimismo, también considera la protección de la información de los dispositivos personales de los usuarios.

Con lo anterior es posible entender que dentro de la seguridad informática se ven involucrados muchos aspectos, aunque con la era digital que se vive actualmente es mucho más fácil ser víctimas de los ataques que implican medios electrónicos.

Si las organizaciones tienen buenas estrategias de seguridad serán más atractivas para los usuarios, ya que éstos adquirirán sus productos o servicios, y la organización tendrá como beneficio una buena reputación, contrariamente a lo que pasaría con las organizaciones que son vulneradas por tener brechas de seguridad donde la información que manejan se ve comprometida.

Como se puede observar, el impacto de la seguridad informática en el ámbito social es muy grande, puesto que le ayuda a todo tipo de organizaciones y a la población en general a realizar diferentes tipos de actividades de manera segura, entre ellos: compartir información, adquirir u ofrecer productos y servicios, comunicarse con personas de prácticamente cualquier parte del mundo o almacenar información. La seguridad informática permite tener una infraestructura segura, donde los usuarios sientan la confianza de compartir información con las organizaciones a los sitios que acceden.

6.7. Impacto económico de la seguridad informática

El uso de los dispositivos de TIC ha provocado que la ciberseguridad juegue un papel importante en la economía de todos los países. Como se ha estado viendo, los dispositivos de TIC actualmente son usados en muchas de las actividades cotidianas, como tomar clases, trabajar de manera remota, para el entretenimiento y estas solo por mencionar algunas, y los ciberdelincuentes buscan errores en la seguridad de los dispositivos y sistemas para ingresar a ellos y realizar actividades delictivas, las cuales afectan negativamente a las víctimas.

Desde el momento en el que las personas y empresas se conectan a internet sus datos están en riesgo, por lo que invertir en la seguridad informática debería ser considerado como una inversión y no como un gasto, sin embargo, pueden darse casos donde invertir en seguridad informática se vea de manera contraria, es decir, se vea como un gasto y no como una inversión, esto provoca que los delitos informáticos se encuentren en el séptimo lugar de las amenazas que tienen un mayor impacto en la economía de todo el mundo de acuerdo con el Informe de Riesgos Globales 2019 desarrollado por el Foro Económico Mundial, publicado en un artículo de la revista Expansión. (Expansión, 2019)

Aunado al creciente uso de la tecnología se suma la situación derivada de la pandemia por COVID-19, muchas empresas, escuelas y personas tuvieron que adaptarse a una vida digital de manera abrupta, pudiendo darse casos en donde no se tenían los recursos o la infraestructura necesaria para realizar labores totalmente en línea.

De acuerdo con el Informe de Amenazas de 2023 realizado por Sophos, una empresa de ciberseguridad, pronosticó que en 2023 el ransomware sería una de las principales amenazas a la seguridad, posteriormente, Kaspersky, una empresa dedicada a la ciberseguridad, realizó un estudio para detectar las amenazas más comunes en pequeñas y medianas empresas en el periodo de enero a mayo de 2023, siendo los exploits el tipo de amenaza más común, en segundo lugar, se encuentran los troyanos y en tercer lugar los backdoors.

Es importante mencionar que de acuerdo con el Informe sobre Riesgos Globales 2024, los avances que se han tenido en el ámbito de la inteligencia artificial también conocida como IA pueden traer consigo grandes consecuencias, esto debido a que los cibercriminales pueden usarlas a su favor para la obtención de información.

Con todo lo anterior se puede comprender la importancia que tiene la ciberseguridad en la economía mundial, por lo que los ciberdelitos afectan a la población de manera general y no solo a las víctimas que son atacadas directamente.

Anteriormente ya se ha mencionado que alcanzar un nivel de riesgo cero es prácticamente imposible, sin embargo, sabiendo la importancia que actualmente tiene la ciberseguridad en la economía mundial es importante que haya expertos que ayuden a evitar que haya más víctimas afectadas por cibercriminales, asimismo, es indispensable saber que hay medidas adicionales

que se pueden tomar para prevenir que los delitos informáticos afecten a la economía, entre los cuales se encuentran:

- En el caso de las empresas y organizaciones es importante valorar el nivel de concientización del personal, para planificar las capacitaciones que deban realizarse, mismas que deben ser de manera continua y permanente al menos una vez al año, en las cuales se den a conocer las buenas prácticas y herramientas que pueden utilizar para mantener un alto nivel de seguridad.
- Después de haber realizado las capacitaciones, se recomienda siempre volver a realizar una valoración del nivel de concientización, para así saber la efectividad de la capacitación realizada y asegurarse que el personal sabrá cómo actuar ante las situaciones de riesgo que se lleguen a presentar.
- Contar con planes preventivos, correctivos y de contingencia para aplicarse cuando sea necesario, intentando disminuir al máximo los posibles riesgos que se puedan presentar.
- Apoyarse de los diversos estándares existentes para mantener la seguridad informática, como la norma ISO 27001.
- Llevar a cabo pruebas de pentesting, que ayuden a determinar los riesgos y vulnerabilidades existentes a fin de disminuirlos antes de que sean explotados por algún ciberdelincuente.
- Realizar auditorías al menos una vez al año, para verificar que los estándares se estén cumpliendo adecuadamente.

Finalmente, es importante recalcar lo importante que es la ciberseguridad tanto para las personas y las organizaciones así como el impacto económico que tiene, ya que que influye directamente en la economía mundial, por lo que la ciberseguridad es un tema que para nada debe tomarse a la ligera, sino al contrario, deben involucrarse a más usuarios para que sean conscientes que la seguridad informática debe verse como una inversión y no como un gasto, lo que ayudará a que disminuyan las pérdidas económicas provocadas por los ciberdelitos.

(Foro Económico Mundial, 2024; Kaspersky, 2023c; Olmos Guarneros, 2022; Ugarte, 2022)

Conclusiones

Estos materiales de estudio para la asignatura de Seguridad Informática Básica cumplen su objetivo principal, ya que tener una fuente confiable de información es de suma importancia para el correcto aprendizaje. El material de estudio fue elaborado tomando como base diferentes fuentes de información, las cuales al complementarse ayudan con el cumplimiento de este objetivo, dentro de estas fuentes de información se encuentran, artículos, investigaciones y tesis, las cuales se encuentran avaladas por distintas universidades o reconocidas organizaciones como Fortinet, IBM o el INEGI, adicionalmente, la asesora del presente trabajo, quien actualmente es la coordinadora del área de redes y seguridad de la Facultad de Ingeniería de la UNAM, tuvo a bien revisar la información contenida, lo cual agrega una capa más de confiabilidad.

Adicionalmente, el profesorado puede hacer uso de este material de estudio como apoyo en la impartición de sus clases, debido a que se apega al plan de estudios de la asignatura en cuestión, asimismo, se brindan materiales audiovisuales como refuerzo de los temas mencionados en la parte documental, y con la sección de reactivos los alumnos podrán poner a prueba lo aprendido.

Se realizó una fase de pruebas donde se tomó un grupo muestra de 49 estudiantes, a quienes se les proporcionaron algunos subtemas del tema 1, titulado “Fundamentos teóricos”, posteriormente se les aplicaron 10 reactivos de un banco de 24 preguntas con relación a los subtemas leídos, como resultado de esta actividad se observó que el promedio del grupo fue aprobatorio, mientras que el tiempo promedio en el que los alumnos resolvieron el cuestionario fue de 9 minutos, esto es un indicador de que la parte documental , el cuestionario y los reactivos tuvieron una redacción clara y entendible, lo cual les ayudó a obtener buenos resultados.

Adicionalmente considero que se alcanzaron beneficios adicionales, puesto que, durante el desarrollo del presente trabajo adquirí conocimiento de diferentes temas relacionados a la seguridad informática, los cuales son útiles para aplicarlos en el ámbito personal y profesional, asimismo, el desarrollo de estos materiales fue un impulso importante en el inicio de mi carrera profesional.

Finalmente, se espera que futuros estudiantes complementen y actualicen estos materiales de estudio para que la validez de su información no se pierda con el paso del tiempo y sigan siendo materiales de apoyo útiles tanto en el aprendizaje de las y los estudiantes de la Facultad de Ingeniería, como para el profesorado que imparte la asignatura. Su frecuencia de actualización dependerá de factores externos, entre ellos las modificaciones al plan de estudios o el surgimiento de nueva información que pueda ser de utilidad o complemente la información del presente trabajo.

Glosario

A

ACL: Access Control List, en español, Lista de Control de Acceso.

ACM: Association for Computing Machinery, y su traducción al español Asociación de Maquinaria Computacional. Es la primera sociedad científica y educativa sobre las ciencias de la computación y afines.

Activos: Bienes y recursos que tiene una organización y que debe proteger.

AEBO: Agencia Estatal Boletín Oficial del Estado, organización que publica, imprime y difunde todo lo que se encuentra en el BOE.

AIEE: American Institute of Electrical Engineers en español conocido como Instituto Americano de Ingenieros Eléctricos.

ALE: Annualized Loss Expectancy o Expectativa de Pérdida Anual. Fórmula con la cual se puede modelar el impacto de los riesgos de seguridad. Expresa la pérdida total monetaria que puede esperar la organización si un riesgo se materializa.

ALG: Application Layer Gateway o Puerta de Enlace de Capa de Aplicación. Componente de software que gestiona protocolos de aplicaciones específicas, como FTP, es como un intermediario entre el internet y un servidor de aplicaciones.

Amenaza: Posibilidad de ocurrencia de un evento accidental o intencionado que ponga en riesgo la seguridad de un sistema.

ANSI: American National Standards Institute, traducido al español como Instituto Nacional Estadounidense de Estándares. Es una organización que supervisa el desarrollo de estándares para productos, procesos y sistemas de EE.UU.

Antimalware: Programa informático que tiene como propósito prevenir, identificar y eliminar software malicioso en los dispositivos.

API: Application Programming Interface o Interfaz de Programación de Aplicaciones. Mecanismo que permite a dos componentes de software comunicarse entre sí.

AP: Access Point o Punto de Acceso. Dispositivo que permite la conexión inalámbrica de dispositivos que se conectan a una red cableada, también permite crear una red inalámbrica externa.

ARO: Tasa de Ocurrencia Anualizada.

ARP: Address Resolution Protocol, en español, Protocolo de Resolución de Direcciones. Se encarga de asociar una dirección IP con su dirección MAC.

ARPA: Advanced Research Projects Network traducido al español como Red de Agencias de Proyectos de Investigación Avanzada.

Ataque: Acción que explota una vulnerabilidad o debilidad.

Auditoría: Revisión de procedimientos llevados a cabo por una empresa u organización, con el fin de verificar que cumple con los requisitos establecidos.

B

Backdoor: Malware que explota una vulnerabilidad para proporcionar a los atacantes acceso remoto al dispositivo infectado.

Backup: Copia de seguridad.

Base64: Algoritmo de codificación que permite representar datos binarios en caracteres del código ASCII.

BIOS: Basic Input - Output System, en español conocido como Sistema Básico de Entrada - Salida, secuencia de código almacenado en memoria ROM, proporciona información sobre los posibles fallos que puedan surgir al iniciar una computadora.

Bit Flipping: Inversión de los bits, es decir, de 1 pasan a 0 y viceversa.

BMIS: Business Model for Information Security, o Modelo de Negocios para la Seguridad de la información.

BOE: Boletín Oficial del Estado, diario donde se publican las leyes y comunicados de manera oficial en España.

Bot: Programa informático que realiza tareas repetitivas de forma automática, imitando el comportamiento humano.

Botnet: Conjunto de computadoras denominadas bots, que son infectadas por algún malware para ser controladas por un ciberdelincuente.

Broadcast: Transmisión de información que se realiza a todos los dispositivos de la red.

Bug: Errores en un programa que producen un comportamiento inesperado.

C

Caché: Memoria que almacena información a la cual se accede varias veces, por lo que la información almacenada ahí puede recuperarse más rápido.

Causahabiente: Heredero que recibe los bienes y derechos cuando fallece el causante.

CC: Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información, también conocidos como Common Criteria o Criterios Comunes.

CCM: Centro de Conmutación Móvil, es la parte central de todo el sistema celular, controla el enrutamiento de las llamadas.

CEI: Computer Ethics Institute, en español, Instituto de Ética Informática.

CEN: Comité Europeo de Normalización.

CENELEC: Instituto Europeo de Normalización Electrotécnica.

CEO: Chief Executive Officer en español conocido como Director Ejecutivo, es decir, es quien ocupa el puesto directivo más alto dentro de una empresa u organización.

CFAA: Computer Fraud and Abuse Act, o Ley de abuso y fraude. Castiga los delitos informáticos en Estados Unidos.

CFO: Chief Financial Officer, en español conocido como Director Financiero. Es el responsable de la planificación económica y financiera de una empresa u organización.

Circuito CCTV: Closed Circuit Television, o Circuito Cerrado de Televisión. Sistema de videovigilancia.

CIS: Center of Internet Security, en español, Centro para la Seguridad de Internet

CLEF: Commercial Licensed Evaluation Facilities o Instalaciones de Evaluación con Licencia Comercial.

CMMI: Capability Maturity Model Integration, en español, Integración de Modelos de Madurez de Capacidades.

CNUDMI: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

COBIT: Control Objectives for Information and Related Technologies, en español, Objetivos de Control para la Información y Tecnologias Relacionadas.

Compilador: Programa que traduce el código escrito en un lenguaje de alto nivel a un lenguaje legible por la máquina o lenguaje de bajo nivel.

Conexiones peer to peer (P2P): Tipo de arquitectura que permite que los dispositivos se comuniquen entre sí sin la necesidad de tener un servidor central.

Consenso: Acuerdo alcanzado por miembros de un mismo grupo.

Concesión: Otorgar a alguien el derecho de explotar un bien durante un tiempo determinado.

Contramedida: Medida que contrarresta los efectos de otra medida.

Controles: Medidas de seguridad implementadas por la organización para prevenir y/o mitigar riesgos.

Cookie: Archivo de datos que se usa para recordar accesos y conocer los hábitos de navegación de los usuarios, también hacen que las páginas web puedan identificar a los dispositivos de los usuarios que han accedido a dichas páginas.

Covert channel: Forma de comunicación mediante un sistema que no fue diseñado para procesos de comunicación.

CPF: Código Penal Federal.

Crack: Software que realiza modificaciones temporales o permanentes a otros softwares, como activar software gratuitamente o autenticar software fraudulento.

CRAMM: CCTA Risk Analysis and Management Method, por su traducción al español, Análisis de Riesgos y Método de Gestión

Criptografía: Algoritmos matemáticos que se usan para cifrar y descifrar información.

CTCPEC: Canadian Trusted Computer Product Evaluation Criteria, por su traducción al español, Criterios de Evaluación de Productos Informáticos de Confianza de Canadá.

CTTA: Central Computer and Telecommunications Agency o Agencia Central de Informática y Telecomunicaciones.

CVE: Common Vulnerabilities and Exposures, en español, Vulnerabilidades y Exposiciones Comunes. identifica unívocamente las vulnerabilidades mediante un código.

CVRF: Common Vulnerability Reporting Framework o Informes de Vulnerabilidad Común, proporciona información precisa al fabricante cuando se cree que se ha encontrado una nueva vulnerabilidad con el fin de que pueda instalar eficazmente las actualizaciones correspondientes.

CVSS: Common Vulnerabilities Scoring System, o Sistema Común de Calificación de los Puntos Vulnerables. Identifica el nivel de gravedad de una vulnerabilidad de software.

D

DBMS: DataBase Management System, en español, Sistema de Gestión de Base de Datos. Software para crear y administrar bases de datos.

DCSSI: Direction Centrale de la Sécurité des Systèmes d'Information o Dirección Central de la Seguridad de los Sistemas de Información

DDoS: Distributed Denial of Service, conocido en español como Ataque Distribuido de Denegación de Servicios. Tipo de ataque que inunda con muchas solicitudes al dispositivo

objetivo desde múltiples dispositivos o direcciones IP, con la finalidad de hacer que el dispositivo objetivo sea incapaz de responder a las solicitudes legítimas.

DHCP: Dynamic Host Configuration Protocol o Protocolo de configuración dinámica de host, permite que los dispositivos adquieran una dirección IP y gateway de manera automática.

Dirección IP: Dirección única que identifica a los dispositivos en internet.

Dirección MAC: Identificador único de 48 bits hexadecimales que le asignan los fabricantes a las NIC de los dispositivos.

DMZ: Demilitarized Zone o Zona Desmilitarizada. Red perimetral que protege a las LAN internas del tráfico no confiable.

DNS: Domain Name Server o Sistema de nombres de dominio. Conjunto de protocolos y servicios que permite usar los nombres de dominio en lugar de las direcciones IP.

DoD: Department of Defense, por su traducción al español, Departamento de Defensa.

DOF: Diario Oficial de la Federación.

DoS: Denial of Service o Denegación de Servicio. Tipo de ataque que inunda con muchas solicitudes al dispositivo objetivo, desde una misma IP, con el objetivo de consumir recursos para que sea incapaz de responder a las solicitudes legítimas.

DSS: Dynamic Spectrum Sharing, en español Compartición Dinámica del Espectro. Permite que los operadores de las redes móviles alternen el uso del espectro radioeléctrico.

E

EB: Estación Base. Recibe y envía señales desde y hacia las estaciones móviles también envía las señales hacía el CCM.

EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité o Expresión de las Necesidades e Identificación de los Objetivos de Seguridad.

ECPA: Electronic Communications Privacy Act o Ley de Privacidad de las Comunicaciones Electrónicas. Ley que protege las comunicaciones, tanto las que se pueden escuchar con el oído humano y las comunicaciones electrónicas.

EDI: Electronic Data Interchange o Intercambio Electrónico de Datos. Intercambio de información entre computadoras.

EIA: Electronic Industries Alliance o Alianza de Industrias Electrónicas, organización que promueve el desarrollo del mercado y competitividad en la industria de la alta tecnología en EE.UU.

EM: Estación Móvil. Teléfono móvil mediante el cual se establecen las llamadas.

Endoso: Proceso legal que permite pasar una deuda de una persona a otra.

ENDUTIH: Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.

Esteganografía: Técnica que sirve para ocultar información en un objeto portador.

Esteganograma: Contenedor que lleva el mensaje oculto a transmitir.

ETH: Ethereum. Tipo de criptomoneda.

Ethernet: Protocolo de red que controla el método de comunicación entre dispositivos.

ETSI: European Telecommunications Standards Institute, en español, Instituto Europeo de Normas de Telecomunicaciones.

Evaluación mixta: Realización de análisis de riesgos cualitativo y cuantitativo.

Exploit: Programa, aplicación o secuencia de comandos que permite a quien lo usa investigar y aprovechar las vulnerabilidades de un sistema.

F

FE: Factor de exposición.

Firewall: Elemento de hardware o software que monitorea el tráfico que pasa a través de una red, además con base en reglas preestablecidas decide el tráfico que deja pasar.

Firmware: Tipo de programa de software que permite controlar y comunicarse con el hardware.

FM: Frecuencia Modulada. Técnica que permite la transmisión de información mediante una onda portadora.

Fonograma: Símbolo que representa un sonido o un grupo de sonidos.

Framework: Conjunto de reglas que se usan para desarrollar software de forma más rápida y eficiente.

FTP: File Transfer Protocol o Protocolo de Transferencia de Archivos, permite transferir archivos entre dispositivos conectados a una red.

G

Gateway: Permite a los dispositivos conectados a él tener acceso a redes exteriores.

H

Hardware: Conjunto de elementos físicos que forman un dispositivo o sistema informático.

Herramientas freeware: Software gratuito, es decir, los usuarios finales pueden adquirirlo sin pagar por él.

Herramientas shareware: Software que pueden adquirir los usuarios finales con funciones limitadas o en una versión de prueba durante un periodo de tiempo determinado.

Hipertexto: Conjunto de textos, gráficos o imágenes interconectados mediante vínculos y conexiones lógicas.

Honeypot: Mecanismo de seguridad que sirve para obtener información sobre los modos de operación de los ciberdelincuentes.

HTML: HyperText Markup Languaje, o Lenguaje de Marcas de Hipertexto. Código que se usa para estructurar y desplegar una página web.

HTTP: Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertextos. Permite cargar páginas web a través de enlaces de hipertexto.

HTTPD: Primer servidor web creado por Tim Berners Lee.

HTTPS: Hypertext Transfer Protocol Secure o Protocolo Seguro de Transferencia de Hipertexto. Permite cargar páginas web a través de enlaces de hipertexto de forma segura.

Hub: Dispositivo de red que permite conectar diferentes nodos entre sí.

I

I&T: Información y Tecnología.

IA: Inteligencia Artificial.

IAM: Indentity and Access Management o Gestión de Identidad y Accesos.

IANA: Internet Assigned Numbers Authority, en español conocida como Autoridad para Números Asignados en Internet. Entidad encargada de asignar las direcciones IP.

ICMP: Internet Control Message Protocol por su traducción al español, Protocolo de mensajes de control de internet. Permite informar problemas con la transmisión de datos.

IDS: Intrusion Detection System o Sistema de Detección de Intrusiones. Monitoriza el tráfico entrante y emite una alerta a los administradores del sistema si detecta alguna actividad sospechosa.

IEC: International Electrotechnical Comission o Comisión Electrotécnica Internacional.

IEEE: Institute of Electrical and Electronics Engineers, en español conocido como Instituto de Ingenieros Eléctricos y Electrónicos. Organización que promueve los avances científicos en las áreas de ingeniería eléctrica, electrónica, informática y afines.

IFAI: Instituto Federal de Acceso a la Información.

IMAP: Internet Message Access Protocol o Protocolo de Acceso a Mensajes de Internet. Permite acceder al correo electrónico desde cualquier dispositivo en cualquier lugar.

Impacto: Pérdida o consecuencia que se ocasiona después de que alguna vulnerabilidad de un activo es explotada.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

INDAUTOR: Instituto Nacional del Derecho de Autor.

INE: Instituto Nacional Electoral.

INEGI: Instituto Nacional de Estadística y Geografía.

Intérprete: Programa informático que procesa el código fuente durante el tiempo de ejecución, procesa el código línea por línea, por lo que lee, analiza y prepara cada secuencia de forma consecutiva para el procesador.

Intranet: Red de comunicación interna de la organización.

IoT: Internet of Things oInternet de las Cosas.

IPS: Intrusion Prevention System, en español, Sistema de Prevención de Intrusiones. Analiza el tráfico de la red para prevenir la ocurrencia de ataques e intrusiones al sistema.

IPSec: Internet Protocol Security o Seguridad de Protocolo en Internet. Conjunto de protocolos que permite la configuración de conexiones seguras a través de una red, mediante el cifrado y la autenticación de cada paquete IP del flujo de datos.

IPv4: IP versión 4, de 32 bits.

IPv6: IP versión 6, de 128 bits.

IRE: Institute of Radio Engineers, por su traducción al español, Instituto de Ingenieros de Radio.

ISA: International Federation of the National Standarizing Associations o Federación Internacional de Asociaciones de Estandarización Nacionales.

ISACF: Información Systems Audit and Control Foundation o Fundación de Auditoria y Control de Sistemas de Información.

ISECOM: Institute for Security and Open Methodologies, en español, Instituto de Seguridad y Metodologías Abiertas. Comunidad de investigación que proporciona recursos, herramientas y certificaciones en el campo de seguridad.

ISO: International Organization for Standardization, en español, Organización Internacional de Normalización.

ISP: Internet Service Provider, en español conocido como Proveedor de Servicios de Internet. Empresas que brindan acceso a internet a los usuarios.

ITAF: Marco de Referencia para el Aseguramiento de la Tecnología de la Información o Information Technology Assurance Framework.

ITIL: Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologias de Información.

ITSEC: Information Technology Security Evaluation Criteria, en español, Criterios de Evaluación de Seguridad en Tecnologias de la Información.

ITSEM: Information Technology Security Evaluation Manual o Manual de Evaluación de la Seguridad de las Tecnologías de la Información.

K

Kernel: También conocido como núcleo, regula la comunicación entre el software y el hardware de la computadora. Es la parte más importante de un sistema operativo.

L

LAN: Local Area Network o Red de Área Local.

Ley SDA: Surveillance Devices Act o Ley de Dispositivos de Vigilancia. Regula el uso de los dispositivos de vigilancia.

Ley TIA: Telecommunication Interception and Access Act o Ley de Acceso e Interceptación de Telecomunicaciones. Ley que protege la privacidad de las comunicaciones.

LFDA: Ley Federal del Derecho de Autor.

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, norma de referencia para la protección de datos en España.

M

MAC: Media Access Control o Control de Acceso a Medios.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

Malware: Software malicioso.

MBR: Master Boot Record o en español Registro de Arranque Maestro. Controla el proceso de arranque de una computadora, contiene información del sistema operativo, como la ubicación de los archivos de arranque y la lista de particiones.

MD5: Message Digest Algorithm o Algoritmo de Resumen de Mensajes. Protocolo criptográfico cuyo propósito es verificar la integridad del contenido de un archivo.

Medios guiados: Son aquellos que conducen las ondas a través de un medio físico, por ejemplo, un cable.

Medios no guiados: Son aquellos que proporcionan un soporte para que las ondas se transmitan, por ejemplo, el aire.

Metasploit: Proyecto de código abierto para encontrar, explotar y validad las vulnerabilidades de un sistema.

Mining: Proceso para adquirir criptomonedas.

MISRA: The Motor Industry Software Reliability Association o Asociación de Fiabilidad del Software en la Industria del Motor.

MITRE: Organización sin fines de lucro que creó un sistema para estandarizar las vulnerabilidades y conocer su gravedad.

Multicast: La transmisión de información se realiza desde un único emisor a un grupo de receptores.

N

NAT: Network Address Translator o Traductor de Direcciones de Red. Traduce una dirección IP privada a una dirección IP pública y viceversa.

NCSC: National Computer Security Center o Centro Nacional de Ciberseguridad.

Nessus: Software de ciberseguridad que sirve para escanear vulnerabilidades de los sistemas operativos.

Nexpose: Software de ciberseguridad que se usa para escanear vulnerabilidades de un sistema o una red.

NEXTSTEP: Sistema Operativo multitarea orientado a objetos desarrollado por NeXT.

NIC: Network Interface Card también conocida como Tarjeta de red. Componente de hardware que proporciona conexiones de red.

NIST: National Institute of Standards and Technology o Instituto Nacional de Estándares y Tecnología.

NMAP: Herramienta de código abierto que se usa para realizar escaneos de red.

No repudio: Servicio de seguridad que permite probar la participación de las partes involucradas en una comunicación.

NSA: National Security Agency o Agencia de Seguridad Nacional.

O

OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation o Evaluación de Amenazas, Activos y Vulnerabilidades Operativamente Criticas.

ONU: Organización de las Naciones Unidas.

OpenVas: Software que permite escanear vulnerabilidades.

OSI: Open System Interconnection, Modelo de Interconexión de Sistemas Abiertos. Modelo de referencia para los protocolos de comunicación de redes.

OSSTMM: Open Source Security Testing Methodology Manual, Manual de Metodología de Pruebas de Seguridad de Código Abierto. Es un estándar que sirve para realizar pruebas de seguridad.

OWASP: Open Web Application Security Project o Proyecto Abierto de Seguridad de Aplicaciones Web.

P

Payloads: Carga maliciosa que ejecuta un hacker en un dispositivo víctima durante un ciberataque.

Pentesting: Ataque malicioso realizado a un sistema de manera controlada con el objetivo de encontrar vulnerabilidades y prevenir posibles fallos.

PHP: Hypertext Preprocessor o Preprocesador de Hipertexto. Lenguaje de programación que permite el desarrollo de aplicaciones web dinámicas.

PIPEDA: Personal Information Protection and Electronic Documents Act, en español, Ley de Protección de Información Personal y Documentos Electrónicos de Canadá. Ley canadiense que regula las acciones que puede llevar a cabo una empresa del sector privado sobre la información personal que manejan.

PKI: Public Key Infrastructure o Infraestructura de Claves Públicas. Permite gestionar y controlar la tarea de generar, validar o revocar certificados digitales.

POP3: Post Office Protocol o Protocolo de Oficina de Correo. Permite que los usuarios descarguen correos electrónicos desde un servidor a un cliente.

PP: Perfil de protección.

Proxy: Intermediario que se ubica entre las peticiones hechas por un cliente a un servidor.

R

RAE: Real Academia Española.

RAID: Redundant Array of Independient Disks, conocido en español como Grupo Redundante de Discos Independientes que tiene como objetivo proteger los datos en caso de que un disco duro falle.

Requerimientos funcionales: Definen lo que un sistema debe realizar para alcanzar las expectativas de los usuarios y satisfacer sus necesidades.

Riesgo: Cualquier amenaza que explote las vulnerabilidades de los activos, provocando pérdidas.

Riesgos residuales: Riesgos de que permanezcan ciertas pérdidas después de implementar los controles para prevenir y/o mitigar los riesgos.

Root: Usuario con mayor control dentro de un sistema.

Rootkit: Software malicioso que permite el acceso no autorizado a los dispositivos.

Router: Dispositivo de red que sirve para enviar y recibir datos en las redes.

RPC: Remote Procedure Call o Llamada a procedimiento remoto. Técnica que usa el modelo cliente – servidor para ejecutar tareas en una máquina remota sin preocuparse por la comunicación.

S

SAMM: Software Assurance Maturity Model o Modelo de Madurez del Aseguramiento del Software.

SAR: Security Assurance Requirement, en español, Requisitos de confianza o aseguramiento.

Script: Fragmento de código cuyo objetivo es añadir funcionalidad.

SEDENA: Secretaría de Defensa Nacional.

SEP: Secretaría de Educación Pública.

SES: Subsecretaría de Educación Superior.

SF: Función de seguridad.

SFP's: Función de las políticas de seguridad.

SFR: Security Functional Requirement o Requisitos Funcionales de Seguridad.

SFTP: Secure File Transfer Protocol, en español, Protocolo de Transferencia Segura de Archivos. Proporciona acceso seguro a un equipo remoto para comunicarse de una forma segura.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIP: Session Initiation Protocol o Protocolo de Inicialización de Sesión. Se usa en VoIP para hacer y recibir llamadas de voz y video.

Sistema EGIT: Gobierno de la Información y Tecnología de las Empresas.

SLE: Expectativa de Pérdida Individual.

SMB: Server Message Block o Bloque de Mensajes del Servidor.

SMS: Short Message Service o Servicio de Mensajes Cortos. Mensaje de texto breve que puede ser enviado entre teléfonos celulares.

SMTP: Simple Mail Transfer Protocol, en español Protocolo para Transferencia Simple de Correo. Se usa en el envío y recepción de correos electrónicos.

Sniffer: Herramienta que permite monitorear el tráfico de la red en tiempo real.

Software: Conjunto de programas informáticos que permite a los dispositivos realizar tareas.

SOGIS: Senior Officials Group Information Systems Security o Grupo de Altos Funcionarios de Seguridad de los Sistemas de Información.

SQL: Structured Query Languaje o Lenguaje de Consulta Estructurada. Lenguaje orientado al manejo de bases de datos.

SRI: Stanford Research Institute o Instituto de Investigación de Stanford

SRTP: Secure Real Time Transport Protocol o Protocolo de Transporte en Tiempo Real Seguro. Protocolo de nivel de aplicación que permite transmitir información en tiempo real.

SSH: Secure Shell, significa Capsula Segura. Protocolo que permite conectarse a un servidor remotamente a través de internet de manera segura.

SSL: Secure Socket Layer o Capa de Sockets Seguros. Protocolo de cifrado anteriormente usado para garantizar la seguridad de los datos en la comunicación realizada a través de internet. Actualmente se usa TLS.

ST: Security Target. Objetivos de seguridad.

Stakeholders: Partes interesadas en un negocio que influyen en la toma de decisiones y además se interesan en los resultados.

Switch: Dispositivo de red que permite conectar diferentes nodos dentro de una red, para que puedan compartir información y comunicarse entre sí.

T

TCP: Transfer Control Protocol conocido en español como Protocolo de Control de Transmisión. Permite que dos hosts se conecten e intercambien datos, además, este protocolo garantiza que los datos fueron entregados en el mismo orden en el que se enviaron.

TCP/IP: Transmission Control Protocol/Internet Protocol, por su traducción al español, Protocolo de control de transmisión/Protocolo de internet. Suite de protocolos que permiten a los dispositivos comunicarse en una red.

TCSEC: Trusted Computer System Evaluation Criteria, en español, Criterios de Evaluación del Sistema Informático de Confianza.

Telégrafo: Dispositivo mediante el cual se transmite información haciendo uso de señales eléctricas transmitidas mediante cables, ondas de radio y un sistema de codificación.

Telegrama: Mensaje transmitido mediante el telégrafo.

Telnet: Telecomunication Network, permite establecer conexiones remotas, actualmente está obsoleto y fue sustituido por SSH.

TI: Tecnologías de Información.

TIA: Telecommunication Industry Association o Asociación de Industrias de Telecomunicaciones. Organización que desarrolla normas de cableado industrial para productos de telecomunicaciones.

TIC: Tecnologías de la Información y las Comunicaciones.

TLS: Transport Layer Security o Capa de Seguridad de Transporte. Protocolo que brinda seguridad a los datos para la comunicación realizada a través de internet.

TOE: Target Of Evaluation, por su traducción al español, Objetivo de Evaluación. Producto o sistema de TI sujeto a una evaluación de seguridad.

TOGAF: The Open Group Architecture Framework o Esquema de Arquitectura del Open Group.

Tráfico de red: Datos que se mueven a través de una red.

Triángulo CID o triada CID: Confidencialidad - Integridad - Disponibilidad.

TSF: Funciones de seguridad del TOE.

TSFI: Interfaces de las funciones de seguridad del TOE.

TSP: Políticas de seguridad del TOE.

TTL: Time To Live o Tiempo de Vida. Tiempo determinado que tienen los datos para ser válidos y estar disponibles en una red.

U

UCLA: University of California at Los Angeles, en español conocida como Universidad de California en los Ángeles.

UDP: User Datagram Protocol, por su traducción al español, Protocolo de datagramas de usuario, permite que dos hosts se conecten e intercambien datos, a diferencia de TCP, este protocolo no garantiza que todos los paquetes se entreguen, ni que se entreguen en el orden en el que fueron enviados.

UNCITRAL: United Nations Commission on International Trade Law, en español CNUDMI.

Unicast: Difusión única, es decir, la transmisión se realiza desde un único emisor a un único receptor.

UNSCC: United Nations Standards Coordinating Committee o Comité Coordinador de Estándares de las Naciones Unidas.

UOC: Universitat Oberta de Catalunya, conocida en español como Universidad Abierta de Cataluña

URL: Uniform Resource Locator o Localizador Uniforme de Recursos. Dirección única que se le asigna a cada recurso existente en la web.

URV: Universitat Rovira i Virgili o Universidad Rovira y Virgili.

USC: United States Code, también conocido como Código de los Estados Unidos.

USCODE: United States Code o Código de los Estados Unidos.

V

VA: Valor del activo.

Videograma: Imágenes asociadas con o sin sonido, que dan la sensación de movimiento.

VLAN: Virtual LAN o Red de Área Local Virtual.

VoIP: Voice over Internet Protocol o Voz sobre Protocolo de Internet. Tecnología que permite realizar llamadas usando internet.

VPN: Virtual Private Network, traducida como Red Privada Virtual. Permite la transmisión de tráfico a través de redes públicas de manera segura.

Vulnerabilidad: Debilidad que puede explotarse para causar daños o pérdidas a un sistema, son el resultado de bugs o fallas en el diseño de un sistema.

Referencias

Access Quality. (2023, julio 17). *4 Tipos de ataques DNS ¿Cómo prevenir?* https://www.accessq.com.mx/tipos-de-ataques-dns/

Acens. (s. f.). *Bases de datos y sus vulnerabilidades más comunes*. https://www.acens.com/comunicacion/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

ACM. (s. f.). *Código de Ética y Conducta Profesional de ACM.* Recuperado 26 de enero de 2024, de https://www.acm.org/about-acm/code-of-ethics-in-spanish

Adyen. (2022, abril 19). *¿Cómo vamos en materia de Protección de Datos en México?* https://www.adyen.com/es_MX/centro-de-informacion/como-vamos-en-materia-de-proteccion-de-datos-en-mexico

AEBOE. (s. f.). *Contenido y secciones del BOE.* Recuperado 25 de enero de 2024, de https://www.boe.es/diario_boe/ayuda.php

Agencia Española Protección Datos. (s. f.). *Fingerprinting o Huella digital del dispositivo.* [Estudio]. https://www.aepd.es/documento/estudio-fingerprinting-huella-digital.pdf

Agencia SINC. (2017, abril 27). *Cómo ocultar información confidencial de forma automática.* https://www.agenciasinc.es/Noticias/Como-ocultar-informacion-confidencial-de-forma-automatica

Agudo, S. (2017, mayo 3). *Phreaking, phreaks y Blue Boxes: Historia del hacking telefónico*. Genbeta. https://www.genbeta.com/a-fondo/phreaking-phreaks-y-blue-boxes-historia-del-hacking-telefonico

Agüero, J. R. (s. f.). Seguridad en la VoIP. *Magazcitum*. Recuperado 19 de enero de 2024, de https://www.magazcitum.com.mx/index.php/archivos/630

Albors, J. (2015, abril 17). *¿Sabes qué es un backdoor y en qué se diferencia de un troyano?* Welivesecurity. https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/

Albors, J. (2020, junio 24). *Qué es un ataque de fuerza bruta y cómo funciona*. Welivesecurity. https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/

Alcántara, A. (2019, agosto 8). *Análisis de Riesgos Cualitativos.* LinkedIn. https://www.linkedin.com/pulse/an%C3%A1lisis-de-riesgos-cualitativos-ang%C3%A9lica-alc%C3%A1ntara/?originalSubdomain=es

Álef. (2017, mayo 7). *Cómo ocultar información confidencial de forma automática en documentos electrónicos.* https://alef.mx/como-ocultar-informacion-confidencial-de-forma-automatica-en-documentos-electronicos/

Alemán Novoa, H., & Rodríguez Barrera, C. (2021). *Metodologías para el análisis de riesgos en los SGSI.* https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/index

Alonso, C. (2015, agosto 3). ISO 27000 y el conjunto de estándares de Seguridad de la Información. *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Alturi, V. (2011). HRU. En *Encyclopedia of Cryptography and Security* (pp. 562-564). Springer US. https://doi.org/10.1007/978-1-4419-5906-5_819

Alvarado Andalón, R., González Nuñez, L., Carballo, M., & Torhtón, M. Á. (s. f.). *Hackeo histórico a servidores de la SEDENA.* Contra la corrupción. Recuperado 21 de enero de 2024, de https://contralacorrupcion.mx/anuario-de-la-corrupcion-2022/hackeo-historico-a-servidores-de-la-sedena

Arcila, J. B. P., Quintero, E. A. F., Aguilar, R., & Mireles, M. (2009). *Ética Informática y Educación Computing Ethics and Education*. *8*. https://www.ugr.es/~sevimeco/revistaeticanet/numero8/Articulos/Formato/articulo2.pdf

Argentina.gob.ar. (2020, diciembre 21). *¿Qué es la ingeniería social y cómo me protejo?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

Australian Goverment. (s. f.). *Telecommunications interception and surveillance.* Recuperado 25 de enero de 2024, de https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance, https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance

Ávila, F. (2018, agosto 8). ¿Qué es un IDS? Tipos, Técnica IDS Evasion y cómo Evitarla. *Disoftin*. http://www.disoftin.com/2018/08/que-es-un-ids-tipos-tecnica-ids-evasion.html

AWS. (s. f.). *¿Qué es DNS?* Amazon Web Services, Inc. Recuperado 19 de enero de 2024, de https://aws.amazon.com/es/route53/what-is-dns/

Ayudaley. (2021, abril 22). *Exploits. Usos, peligros, detección y eliminación.* Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2021/04/22/exploits/

Ballesteros Riveros, P. D., & Calas Sierra, L. D. (2007). *Propuesta de implementación del modelo multinivel Bell-LaPadula en Linux.* [Proyecto de grado., Universidad de los Andes.].

https://repositorio.uniandes.edu.co/server/api/core/bitstreams/3b26bb75-2c6f-4dbb-bef9-bb25a81e8839/content

BBVA. (2024, enero 20). *Conoce cómo prevenir un fraude cibernético y cuántos tipos existen.* https://www.bbva.mx/educacion-financiera/banca-digital/cuenta-digital-fraude-cibernetico.html

Becolve Digital. (2019, noviembre 8). *Estrategia de Defensa en profundidad en ciberseguridad industrial (I)*. https://becolve.com/blog/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/

Belcic, I. (2020a, mayo 14). *¿Qué es un sniffer y cómo puede protegerse?* Academy. https://www.avast.com/es-es/c-sniffer

Belcic, I. (2020b, octubre 22). *¿Qué es un exploit en seguridad informática?* ¿Qué Es Un Exploit En Seguridad Informática? https://www.avg.com/es/signal/computer-security-exploits

Bello, E. (2023). Ciberseguridad: Tipos de ataques y en qué consisten. *Thinking for Innovation*. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Biblioteca del Congreso Nacional de Chile. (2014, noviembre 27). *Delitos informáticos.* [Text]. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/portal/leyfacil/recurso/delitos-informaticos

Billin. (s. f.). *¿Qué es el Activo de una empresa?* Recuperado 21 de enero de 2024, de https://www.billin.net/glosario/definicion-activo/

Bituser. (2016, octubre 7). 8 Pasos sobre la instalación de servidores—Bits empresa de ti mexico. *BITS.* https://bits.com.mx/8-pasos-sobre-instalacion-de-servidores/

BJA. (s. f.). *Electronic Communications Privacy Act of 1986 (ECPA).* Recuperado 25 de enero de 2024, de https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Bodnar, D. (2020, octubre 29). *Ingeniería social y cómo protegerse*. Avast. https://www.avast.com/es-es/c-social-engineering

Borghello, C. (s. f.). *Legislación y Delitos Informáticos.* Segu-Info. Recuperado 25 de enero de 2024, de https://www.segu-info.com.ar

Borreda, L. (2021, julio 21). *Qué es el «dumpster diving» y cómo prevenir este ataque*. Red Seguridad. https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-dumpster-diving-y-como-prevenir-este-ataque_20210721.html

BSI Group. (s. f.). *¿Qué es una norma? -Ventajas y Beneficios para su uso*. Recuperado 13 de enero de 2024, de https://www.bsigroup.com/es-MX/normas/Informacion-acerca-de-las-normas-/Que-es-una-norma/

Burdova, C. (2021, junio 22). *¿Qué es un rootkit?* ¿Qué es un rootkit y cómo se elimina? https://www.avast.com/es-es/c-rootkit

Bustamante Sánchez, R. (s. f.). *Seguridad en redes.* [Monografía., Universidad Autónoma del Estado de Hidalgo.]. https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

Calderón Arateco, L. L. (s. f.). *Seguridad informática y seguridad de la información* [Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00002658.pdf

Cano Rubio, I. (2018, febrero 21). *Tipos de seguridad informática*. Viewnext. https://www.viewnext.com/tipos-de-seguridad-informatica/

Carmona Dávila, D. (s. f.). *España reconoce oficialmente la Independencia de México mediante el Tratado "Santa María-Calatrava".* Memoria Política de México. Recuperado 21 de enero de 2024, de https://www.memoriapoliticademexico.org/Efemerides/12/28121836.html

Carrillo Jiu, J. A. (2014). *Fundamentos de seguridad lógica.* [Informe de trabajo práctico de suficiencia., Universidad Nacional de la Amazonia Peruana.]. https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/4487/Jose_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y

Carvajal Herrera, R. D. (2013). *Seguridad informática y de información* [Universidad Tecnológica de Bolivar]. https://biblioteca.utb.edu.co/notas/tesis/0065029.pdf

CaseGuard. (2022a, junio 29). *La Ley de Fraude y Abuso Informático de 1986.* https://caseguard.com/es/articles/la-ley-de-fraude-y-abuso-informatico-de-1986/

CaseGuard. (2022b, julio 19). *La Ley Patriota, el terrorismo y la preocupación por la privacidad global.* https://caseguard.com/es/articles/la-ley-patriota-el-terrorismo-y-la-preocupacion-por-la-privacidad-global/

Cassou Ruiz, J. E. (s. f.). *Delitos informáticos en México*. https://escuelajudicial.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

Castillo Maza, J. (2003, mayo 10). *Gestión de seguridad de los sistemas de información*. https://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/administracion/v05_n10/gestion.htm

Castillo, J. A. (2019, enero 20). Telnet qué es y para qué sirve. *Profesional Review*. https://www.profesionalreview.com/2019/01/20/telnet-que-es/

CC Portal. (2013). *Common Criteria History*. https://www.commoncriteriaportal.org/iccc/ICCC_arc/history.htm

CCN CERT. (s. f.-a). *Criterios comunes*. Recuperado 13 de enero de 2024, de https://www.dit.upm.es/~pepe/401/index.html#!3479

CCN CERT. (s. f.-b). *ITSEC - Information Technology Security Evaluation Criteria*. Recuperado 13 de enero de 2024, de https://www.dit.upm.es/~pepe/401/index.html#!5112

CCN CERT. (s. f.-c). *Modelo de Bell-LaPadula.* Recuperado 21 de enero de 2024, de https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=614.html

Centro de Estudios y Servicios en Salud. (s. f.). *Psicología.* Recuperado 26 de enero de 2024, de https://www.uv.mx/veracruz/cess/vinculacion-y-extension/psicologia/

Chamorro Lopez, J. A. (2011). *Modelo para la Evaluación en Seguridad Informática a Productos Software, basado en el Estándar ISO/IEC 15408 Common Criteria* [Universidad Icesi]. https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/67925/1/modelo_evaluacion_seguridad.pdf

Ciberpyme. (2021a, noviembre 11). Tipos de ciberataques: Ataque a contraseñas. *CiberseguridadPYME.* https://www.ciberseguridadpyme.es/actualidad/ataque-a-contrasenas/

Ciberpyme. (2021b, diciembre 9). *Tipos de ciberataques: Ataques a las conexiones inalámbricas.* https://www.ciberseguridadpyme.es/actualidad/ataques-a-las-conexiones/

Ciberseguridad. (s. f.-a). *Análisis de vulnerabilidades.* Recuperado 20 de enero de 2024, de https://ciberseguridad.com/servicios/analisis-vulnerabilidades/

Ciberseguridad. (s. f.-b). *Dumpster Diving*. Recuperado 19 de enero de 2024, de https://ciberseguridad.com/amenzas/dumpster-diving/

Ciberseguridad. (s. f.-c). *Ingeniería social inversa*. Recuperado 14 de enero de 2024, de https://ciberseguridad.com/amenzas/ingenieria-social-inversa/

Ciberseguridad. (s. f.-d). *Normativa de Ciberseguridad en España*. Recuperado 25 de enero de 2024, de https://ciberseguridad.com/normativa/espana/

Ciberseguridad. (s. f.-e). *¿Qué es Metasploit Framework y cómo funciona?* Recuperado 20 de enero de 2024, de https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Ciberseguridad. (s. f.-f). *¿Qué es OSSTMM? Definición, historia y características*. Recuperado 20 de enero de 2024, de https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/

Cilli, C. (2017, octubre 25). *Understanding Covert Channels of Communication*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/understanding-covert-channels-of-communication

CILSA. (s. f.). *¿Qué es un sistema operativo?* Recuperado 19 de enero de 2024, de https://desarrollarinclusion.cilsa.org/tecnologia-inclusiva/que-es-un-sistema-operativo/

Cisco. (s. f.-a). *¿Qué es la seguridad de red?* Recuperado 14 de enero de 2024, de https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Cisco. (s. f.-b). *¿Qué es una red inalámbrica?* Recuperado 19 de enero de 2024, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html

Cloudflare. (s. f.). *¿Qué es DNS? Cómo funciona*. Recuperado 19 de enero de 2024, de https://www.cloudflare.com/es-es/learning/dns/what-is-dns/

Código Penal Federal [C.P.F.]. Reformado, Diario Oficial de la Federación [D.O.F.], 14 de agosto de 1931. (México). https://docs.mexico.justia.com/federales/codigo-penal-federal.pdf

Cofide. (2019, marzo 23). *¿Qué protege el derecho de autor y cuáles son sus características?* https://www.cofide.mx/blog/que-protege-el-derecho-de-autor-y-cuales-son-sus-caracteristicas

Colorado Ángel, P. J., & Torres Baquero, I. J. (2015). *Análisis de seguridad de aplicaciones móviles nativas para el sistema operativo android.* [Universidad Nacional Abierta y a Distancia.]. https://1library.co/article/unidos-marco-legal-an%C3%A1lisis-seguridad-aplicaciones-m%C3%B3viles-nativas.q0665exq

Comisión de Derechos Humanos del Estado de México. (s. f.). *Código Hammurabi.* [CODHEM]. Comisión de Derechos Humanos del Estado de México. Recuperado 26 de enero de 2024, de https://www.codhem.org.mx/codigo-hammurabi/

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s. f.). *¿Sabes qué es el Robo de Identidad?* gob.mx. Recuperado 20 de enero de 2024, de http://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad

Computer Professionals For Social Responsibility. (2011, septiembre 1). *The Ten Commandments of Computer Ethics* [Web Page]. http://cpsr.org/issues/ethics/cei/

Consejo General del Trabajo Social. (2016). *¿Qué son los colegios profesionales y para qué sirven?* [Guía]. https://www.cgtrabajosocial.es/app/webroot/files/consejo/files/GUIA_COLEGIACION.pdf

Copro. (s. f.). *Activo (seguridad informática).* Recuperado 21 de enero de 2024, de https://copro.com.ar/Activo_(seguridad_informatica).html

Cortes Monroy, H. (2002). *Certificación del nivel de seguridad en aplicaciones*. https://repositorio.tec.mx/handle/11285/628402

Crecer. (2018, enero 3). *Misión y visión de la empresa. ¿Por qué son importantes?* https://www.crecer.cl/importancia-mision-vision-empresas/

Cruzito, R. R. (2020, noviembre 14). Cálculos de evaluación de riesgos de seguridad informática: SLE, ALE y ARO. *Estudyando*. https://estudyando.com/calculos-de-evaluacion-de-riesgos-de-seguridad-informatica-sle-ale-y-aro/

Cyberseguridad.net. (2021, febrero 27). *NAT Slipstreaming (Ataques informáticos XIII).* https://www.cyberseguridad.net/nat-slipstreaming-ataques-informaticos-xiii

Dávila, J. (2009). *Los límites de la confianza en la certificación de seguridad de productos y sistemas*. *86*. https://revistasic.com/revista86/pdf_86/sic86_enconstruccion.pdf

DBpedia. (s. f.). *Canadian Trusted Computer Product Evaluation Criteria*. Recuperado 13 de enero de 2024, de https://dbpedia.org/page/Canadian_Trusted_Computer_Product_Evaluation_Criteria

DCSSI. (2004). *EBIOS.* https://docplayer.es/12500122-Compendio-ebios-version-del-4-de-febrero-de-2004.html

De la Cruz, H. (2021, septiembre 9). Metodología OCTAVE para el análisis de riesgos en SGSI. *Grupo ESGinnova.* https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

Del Prado, J. (2013, noviembre 22). *Concepto de Norma de Seguridad*. Blog de PRL - IMF Smart Education. https://blogs.imf-formacion.com/blog/prevencion-riesgos-laborales/actualidad-laboral/concepto-de-norma-de-seguridad/

Delgado Avenia, C. A. (2017). *Fundamentos de seguridad informática*. https://core.ac.uk/download/pdf/326424171.pdf

Delgado Granados, M. de L. (s. f.). *Delitos informáticos. Delitos Electrónicos.* http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Dorian. (2020, enero 8). ¿Cómo Funciona un Teléfono Inalámbrico? *Electrónica Básica*. https://electronica-basica.com/telefono-inalambrico/

DragonJAR. (2008, septiembre 20). *Proyectos OWASP en español.* https://www.dragonjar.org/proyectos-owasp-en-espanol.xhtml

DragonJAR. (2010, diciembre 4). *OSSTMM (Open Source Security Testing Methodology Manual) 3.0.* https://www.dragonjar.org/osstmm-open-source-security-testing-methodology-manual-3-0.xhtml

DragonJAR. (s. f.). *Programación Segura—DragonJAR*. Recuperado 19 de enero de 2024, de https://www.dragonjar.org/programacion-segura

DWheeler. (s. f.). *Flawfinder.* Recuperado 19 de enero de 2024, de https://dwheeler.com/flawfinder/

EISF. (2014). *Seguridad de las instalaciones.* [Guía del EISF]. https://gisf.ngo/wp-content/uploads/2018/01/Mo%CC%81dulo-7.pdf

El Economista. (2022, julio 3). *La Estrategia Nacional de Ciberseguridad en México tiene más motivos económicos que de protección de datos: OEA*. https://www.eleconomista.com.mx/tecnologia/La-Estrategia-Nacional-de-Ciberseguridad-en-Mexico-tiene-mas-motivos-economicos-que-de-proteccion-de-datos-OEA-20220703-0001.html

El Tiempo. (1994, mayo 24). *QUÉ ES LA TELEFONÍA CELULAR*. https://www.eltiempo.com/archivo/documento/MAM-135410

Emaint. (2021, abril 28). *¿Qué es el mantenimiento preventivo?* https://www.emaint.com/es/what-is-preventive-maintenance/

Embajada de México en Austria. (2016, septiembre 5). *Objetivos de la CNUDMI.* https://embamex.sre.gob.mx/austria/index.php/es/mision-de-mexico-onu/cnudmi/objetivos

Encyclopedia by Kaspersky. (s. f.). *Las vulnerabilidades de software*. Recuperado 20 de enero de 2024, de https://encyclopedia.kaspersky.es/knowledge/software-vulnerabilities/

Encyclopedia.com. (s. f.). *Computer Ethics Institute.* Recuperado 26 de enero de 2024, de https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/computer-ethics-institute

Equipo Coremain. (2021, octubre 15). *Principales vulnerabilidades de software y cómo solucionarlas*. Coremain. https://www.coremain.com/vulnerabilidades-software/

Escuela Europea de Excelencia. (2019, mayo 8). *Aclaraciones importantes acerca del riesgo residual en ISO 27001.* https://www.escuelaeuropeaexcelencia.com/2019/05/aclaraciones-importantes-acerca-del-riesgo-residual-en-iso-27001/

eSemanal. (2022, agosto 24). *Fortinet registró 85 mil millones de intentos de ciberataques en México, es el país más atacado de la región*. https://esemanal.mx/2022/08/fortinet-registro-85-mil-millones-de-intentos-de-ciberataques-en-mexico-es-el-pais-mas-atacado-de-la-region/

Eset. (s. f.). *¿Qué es un Troyano informático?* Recuperado 21 de enero de 2024, de https://www.eset.com/es/caracteristicas/malware-troyano/

Etxahun. (s. f.). *Metodología de Programación Segura: Herramientas para minimizar el riesgo asociado.* Recuperado 19 de enero de 2024, de https://etxahun.gitbooks.io/seguridad-en-sistemas-de-control-y-automatizacion/content/metodologia_de_programacion_segura_herramientas_pa.html

Euroinnova Business School. (s. f.). *¿Qué es la ética informática?* Recuperado 26 de enero de 2024, de https://www.euroinnova.mx/blog/que-es-la-etica-informatica

Expansión. (2019, febrero 20). *Los ciberataques están entre las amenazas de mayor impacto para la economía.* https://expansion.mx/economia/2019/02/19/los-ciberataques-estan-entre-las-amenazas-de-mayor-impacto-para-la-economia

F5, Inc. (s. f.). *¿Qué es el envenenamiento de cookies?* Recuperado 21 de enero de 2024, de https://www.f5.com/es_es/glossary/cookie-poisoning

Federal Trade Comission Consumer Advice. (2021, marzo 17). *What To Know About Identity Theft*. Consumer Advice. https://consumer.ftc.gov/articles/what-know-about-identity-theft

Fernandez, E. (2019a, abril 5). ¿Qué es un Firewall de next-generation? *CiberseguridadPYME*. https://www.ciberseguridadpyme.es/aprende-ciberseguridad/formacion-basica-para-usuarios/que-es-un-firewall-de-next-generation/

Fernandez, E. (2019b, abril 29). ¿Qué es un Pentester o Pentesting? ¿Cómo funciona? *CiberseguridadPYME.* https://www.ciberseguridadpyme.es/aprende-ciberseguridad/formacion-basica-para-usuarios/que-es-un-pentester-o-pentesting-como-funciona/

Fernández, G. (2018, junio 27). *El concepto de riesgo, probabilidad e impacto de la evaluación de impacto de protección de datos.* Iberley. https://www.iberley.es/revista/concepto-riesgo-probabilidad-impacto-evaluacion-impacto-proteccion-datos-219

Fernández, Y. (2020, mayo 5). *BOE Online: Qué es y cómo usarlo para encontrar lo que buscas.* Xataka. https://www.xataka.com/basics/boe-online-que-como-usarlo-para-encontrar-que-buscas

Fidetia. (2015, abril 30). *Política de seguridad*. https://www.fidetia.es/politica_seguridad.php

Filgueiras Nodar, J. M. (2017). *La ética de los profesionales de la informática en códigos internacionales y mexicanos* [Artículo]. Universidad del Mar, campus Huatulco. https://www.researchgate.net/publication/322834897_La_etica_de_los_profesionales_de_la_informatica_en_codigos_internacionales_y_mexicanos

Foro Económico Mundial. (2024, enero 10). *Riesgos Globales 2024: Los riesgos aumentan, pero también nuestra capacidad de respuesta.* https://es.weforum.org/agenda/2024/01/informe-sobre-riesgos-globales-2024-los-riesgos-aumentan-pero-tambien-nuestra-capacidad-de-respuesta/

Foro Histórico de Telecomunicaciones. (s. f.). *BERNERS-LEE, Timothy*. Recuperado 19 de enero de 2024, de https://forohistorico.coit.es/index.php/personajes/personajes-internacionales/item/berners-lee-timothy

Fortra. (2018, julio 12). *Cómo establecer una política de ciberseguridad*. https://www.fortra.com/es/blog/como-crear-una-politica-de-ciberseguridad-para-su-empresa

F-Secure. (s. f.). *¿Qué es un troyano?* Recuperado 21 de enero de 2024, de https://www.f-secure.com/es/articles/what-is-a-trojan

Fuentes Rivera, S. (2023, enero 18). *Ley de Ciberseguridad en México: Conoce la Nueva Ley*. Delta Protect. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico

García, D. (2023, mayo 4). Ataque: Qué es, características, tipos. *MSMK*. https://msmk.university/ciberseguridad/ataque

Garijo, M. (2019, junio 4). *Garantizar la seguridad de las instalaciones de la empresa*. Expense Reduction Analysts. https://lat.expensereduction.com/noticias/garantizar-seguridad-instalaciones-empresa/

GCFGlobal.org. (s. f.). *Informática Básica: ¿Qué es hardware y software?* Recuperado 19 de enero de 2024, de https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/

GeeksforGeeks. (2020, noviembre 24). *14 Most Common Network Protocols And Their Vulnerabilities*. https://www.geeksforgeeks.org/14-most-common-network-protocols-and-their-vulnerabilities/

Ginzo. (2021, noviembre 17). *Pentesting: Qué es, Tipos y Proceso*. https://ginzo.tech/pentesting/

GlobalSuite Solutions. (2021, junio 17). *Cómo considerar los controles en la estrategia de gestión de riesgos.* https://www.globalsuitesolutions.com/es/como-considerar-controles-estrategia-gestion-de-riesgos/

GlobátiKa. (2019, agosto 23). *Metodología OSSTMM*. https://peritosinformaticos.es/metodologia-osstmm/

Gobierno de Colombia. (s. f.). *Organización de las Naciones Unidas (ONU).* Cancillería. Recuperado 22 de enero de 2024, de https://www.cancilleria.gov.co/organizacion-las-naciones-unidas-onu

Gobierno de México. (s. f.). *México en la ONU*. Embamex. Recuperado 22 de enero de 2024, de https://embamex.sre.gob.mx/filipinas/index.php/servicios-consulares/servicios-a-mexicanos?id=98:mexicoonu

Gobierno del Estado de Tabasco. (s. f.). *Guia para aplicar la Norma TIA/EIA 568 para cableado estructurado.* [Guia]. https://tabasco.gob.mx/sites/default/files/Manual-para-aplicar-la-norma-TIA-EIA-para-Cableado-Estructurado.pdf

Gómez, H. (2015, abril 28). *¿Cuáles son las principales amenazas de seguridad para el hardware?* CSO España. https://cso.computerworld.es/tendencias/cuales-son-las-principales-amenazas-de-seguridad-para-el-hardware

González, A. (2018, enero 15). *Plan de contingencia.* Emprendepyme. https://emprendepyme.net/plan-de-contingencia.html

Gonzalez, P. (2020, noviembre 16). COBIT 2019—El nuevo modelo de gobierno empresarial para información y tecnología. *Medium*. https://ppglzr.medium.com/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b

GovInfo. (s. f.). *United States Code*. Recuperado 25 de enero de 2024, de https://www.govinfo.gov/app/collection/https%3A%2F%2Fwww.govinfo.gov%2Fapp%2Fcollection%2Fuscode

GraphEverywhere, E. (2020, enero 28). *Reportes sobre riesgo | Análisis de Riesgo.* https://www.grapheverywhere.com/reportes-sobre-riesgo/

Grupo ACMS Consultores. (s. f.). *Análisis de Riesgos: Clave para una Gestión Eficaz.* Recuperado 21 de enero de 2024, de https://www.grupoacms.com/consultora/analisis-de-riesgos-en-trabajo

Grupo Atico34. (2020a, mayo 12). *Qué es la criptografía asimétrica y cómo funciona.* https://protecciondatos-lopd.com/empresas/criptografia-asimetrica/

Grupo Atico34. (2020b, mayo 14). *¿Qué es un backdoor y cómo eliminarlo?* https://protecciondatos-lopd.com/empresas/backdoor/

Grupo Atico34. (2020c, junio 17). *Los 10 mejores firewall o cortafuegos para Windows*. https://protecciondatos-lopd.com/empresas/mejores-firewall-windows/

Grupo Atico34. (2021a, mayo 11). *Vulnerabilidad informática: Qué es y cómo protegerse.* https://protecciondatos-lopd.com/empresas/vulnerabilidad-informatica/

Grupo Atico34. (2021b, julio 1). *Escaneo de puertos. ¿Para qué se hace?* https://protecciondatos-lopd.com/empresas/escaneo-de-puertos/

Grupo Atico34. (2023, abril 5). *Ley de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) 2018.* https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/

Grupo ESGinnova. (2013, agosto 14). La ISO 27001. Origen y evolución. *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

Grupo ESGinnova. (2015, julio 26). Origen de las normas ISO. *Software ISO*. https://www.isotools.us/2015/07/26/origen-normas-iso/

Guerrero, G. (2020, septiembre 30). Análisis Cualitativo: [Métodos, Concepto, Ejemplos]. *Autorizado Red.* https://www.autorizadored.es/finanzas/analisis-cualitativo/

Guijarro Rodríguez, A. A., Yepez Holgin, J. M., Peralta Guaraca, T. J., & Ortiz Zambrano, M. (2018). *Defensa en profundidad aplicado a un entorno empresarial*. *39*(42). https://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

Hernández, G. (2021, noviembre 17). *Códigos de ética en el trabajo, ¿por qué son importantes y qué deben contener?* El Economista. https://www.eleconomista.com.mx/capitalhumano/Codigos-de-etica-en-el-trabajo-por-que-son-importantes-y-que-deben-contener-20211116-0097.html

Herramientas WEB. (s. f.). *El protocolo IP*. Recuperado 21 de enero de 2024, de https://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html

Herrera, E., García, J., Fonseca, L., Hernández, F., Néstor, I., & Oscar, L. (2012). *Modelo de Seguridad Clark-Wilson.* [Especialización en seguridad informática., Universidad Piloto de Colombia.]. https://pdfslide.tips/documents/modelo-de-seguridad-clark-wilson.html

HN. (2020, noviembre 5). ¿Qué es una Base de Datos? ¿para qué sirven? *HN Datacenter*. https://www.hn.cl/blog/para-que-sirven-la-bases-de-datos/

Hofmann, M. T. (2021, mayo). *El perfil de los piratas informáticos, la psicología detrás del ciberdelito.* TED. https://www.ted.com/talks/mark_t_hoffmann_profiling_hackers_the_psychology_of_cybercrime/transcript?language=es

Hosting Perú. (2017, febrero 20). *¿Qué son los ataques informáticos?* https://www.hn.pe/blog/que-son-los-ataques-informaticos/

HP. (2021, mayo 3). *¿Qué es el BIOS en tu PC? Para qué sirve y su configuración*. https://www.hp.com/mx-es/shop/tech-takes/como-acceder-a-la-configuracion-del-bios-en-una-pc-con-windows

IBM. (2014). *Redes Sistema de nombres de dominio (DNS).* https://www.ibm.com/docs/es/ssw_ibm_i_72/rzakk/rzakkpdf.pdf

IBM. (2023, octubre 10). *Política y objetivos de seguridad.* https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

IBM. (s. f.). *¿Qué es Smishing (SMS Phishing)?* Recuperado 14 de enero de 2024, de https://www.ibm.com/mx-es/topics/smishing

IEC. (s. f.). *IEC*. Recuperado 13 de enero de 2024, de https://www.iec.ch/homepage

IEEE Sección España. (s. f.). *Quienes Somos*. Recuperado 26 de enero de 2024, de https://ieeespain.org/quienes-somos/

IEEE/ACM. Código de Ética y ejercicio profesional de ingeniería de software. Versión 5.2. https://www.u-cursos.cl/ingenieria/2009/2/CC50M/1/material_docente/bajar?id_material=242547

Imperva. (s. f.). What is an HTTP Flood attack. *Learning Center*. Recuperado 21 de enero de 2024, de https://www.imperva.com/learn/ddos/http-flood/

INAI. (2016). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* [Guía.]. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf

INAI. (s. f.). *Guía para prevenir el robo de identidad.* [Guía]. https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Gu%C3%ADa_Prevenir_RI.pdf

INAI. (s. f.-a). *Normativa y legislación en PDP. Leyes en México para la protección de datos personales.* Recuperado 22 de enero de 2024, de https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

INAI. (s. f.-b). *¿Qué es el INAI?* Recuperado 22 de enero de 2024, de https://home.inai.org.mx/?page_id=1626

INCIBE. (2019a, julio 4). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas.* https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

INCIBE. (2019b, septiembre 5). *Ingeniería social: Técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

INDAUTOR. (s. f.). *Derechos de autor.* https://www.indautor.gob.mx/documentos/informacion-general/Derecho_de_autor.pdf

Infobae México. (2023, julio 2). *La grave vulnerabilidad que puede vivir México, el INAI urgió Ley de Ciberseguridad*. https://www.infobae.com/mexico/2023/07/02/la-grave-vulnerabilidad-que-puede-vivir-mexico-el-inai-urgio-ley-de-ciberseguridad-esta-desactualizado/

Institut Sa Palomera. (s. f.). *Seguridad de switches: Administración e implementación*. Recuperado 21 de enero de 2024, de https://www.sapalomera.cat/moodlecf/RS/2/course/module2/2.2.2.2/2.2.2.2.html

Instituto Nacional de Tecnologías de la Comunicación. (s. f.). *¿Qué son las vulnerabilidades del software?* [Cuaderno de notas.]. https://www.jesusamieiro.com/wp-content/uploads/2011/08/Que_son_las_vulnerabilidades_del_-software.pdf

Interpol. (s. f.). *Cryptojacking*. Recuperado 21 de enero de 2024, de https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

Iriarte Medina, J. (2006). *Estandares para la seguridad de información con tecnologias de información* [Universidad de Chile]. https://repositorio.uchile.cl/bitstream/handle/2250/108414/medina_j.pdf?sequen

ISACA. (2018). *COBIT 2019*. https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

ISECOM. (s. f.). *OSSTMM 3. The Open Source Security Testing Methodology Manual.* https://www.isecom.org/OSSTMM.3.pdf

ISO 27001. (s. f.). *Referencias Normativas ISO 27000*. Recuperado 13 de enero de 2024, de https://normaiso27001.es/referencias-normativas-iso-27000/

ISO. (s. f.). *ISO/IEC TR 15942:2000*. Recuperado 19 de enero de 2024, de https://www.iso.org/standard/29575.html

ISO27000. (s. f.). *Serie 27000*. Recuperado 13 de enero de 2024, de https://www.iso27000.es/iso27000.html

IT Perfection. (2020, julio 25). *OS Fingerprinting*. https://www.itperfection.com/network-security/os-fingerprinting-active-passive-firewall-hacking-cybersecurity-network-security-tcp-nmap-xprobe2-ettercap-p0f/, https://www.itperfection.com/network-security/os-fingerprinting-active-passive-firewall-hacking-cybersecurity-network-security-tcp-nmap-xprobe2-ettercap-p0f/

Jiménez Jiménez, C. (s. f.). *Seguridad en redes y sistemas. Técnicas y conceptos sobre hacking y pentesting.* [Trabajo final de grado., Universidad Oberta de Catalunya].

Recuperado 20 de enero de 2024, de https://1library.co/document/ye1o2v4z-asedios-cibern%C3%A9ticos-t%C3%A9cnicas-conceptos-hacking-pentesting-memoria-copyright.html

Jiménez, J. (2021a, abril 22). *Cómo podrían atacarnos a través de una red Wi-Fi*. RedesZone. https://www.redeszone.net/tutoriales/redes-wifi/ataques-mediante-red-wifi/

Jiménez, J. (2021b, agosto 1). *Ataques DNS: qué son y cómo protogernos*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/consejos-evitar-ataques-dns/

Jiménez, J. (2022, marzo 20). *Qué es un hacker de sombrero gris y cómo actúa.* RedesZone. https://www.redeszone.net/tutoriales/seguridad/que-es-hacker-sombrero-gris/

Jimenez, M. (2018, octubre 8). *¿Qué es un código deontológico?* Cursos.com. https://cursos.com/blog/codigo-deontologico/

Jiménez, M. M. (2021, septiembre 1). *Frecuencia e impacto en la matriz de riesgos.* https://www.piranirisk.com/es/blog/matriz-de-riesgos-frecuencia-impacto

José, M. (2022, enero 11). Ética informática ¿Qué es y cómo influye en el desarrollo de nuevas tecnologías? *Internet Paso a Paso*. https://internetpasoapaso.com/etica-informatica/

Junta de Andalucia. (s. f.-a). *Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM).* Recuperado 20 de enero de 2024, de https://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

Junta de Andalucia. (s. f.-b). *PMD y la calidad estática del código.* Recuperado 19 de enero de 2024, de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/374

Justia. (2020, agosto 26). *Preguntas y Respuestas Sobre Delitos Informáticos*. https://mexico.justia.com/derecho-penal/delitos-informaticos/preguntas-y-respuestas-sobre-delitos-informaticos/

Justia. (2023, mayo 25). *Código Penal Federal*. https://mexico.justia.com/federales/codigos/codigo-penal-federal/

Kaspersky. (2023a, abril 19). *¿Qué es la inyección de SQL? Definición y explicación*. https://latam.kaspersky.com/resource-center/definitions/sql-injection

Kaspersky. (2023b, abril 19). *¿Qué es un keylogger?* https://latam.kaspersky.com/resource-center/definitions/keylogger

Kaspersky. (2023c, junio 27). *How cybercrime is impacting SMBs in 2023.* Securelist. https://securelist.com/smb-threat-report-2023/110097/

Kaspersky. (2024, enero 18). *¿Qué es la ingeniería social?* https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kelnet Computer. (2021, agosto 2). *Seis tipos de ataques a contraseñas: Métodos de ataque y contramedidas.* https://kelnetcomputer.com/seis-tipos-de-ataques-a-contrasenas-metodos-de-ataque-y-contramedidas/

KIO One Step Forward. (s. f.). *¿Qué son y para qué sirven los protocolos de comunicación de redes?* Recuperado 21 de enero de 2024, de https://www.kio.tech/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes

Latto, N. (2016, agosto 11). *¿Qué son los keyloggers y cómo funcionan?* Avast. https://www.avast.com/es-es/c-keylogger

Leal, M. (2012). *Principios de la Seguridad Informática*. https://2asirseguridadinformatica.files.wordpress.com/2013/11/principios-de-la-seguridad-informc3a1tica.pdf

Learn Microsoft. (2023, marzo 14). *Hardware Errors and Error Sources*. https://learn.microsoft.com/en-us/windows-hardware/drivers/whea/hardware-errors-and-error-sources

Lemus, J. (2020, febrero 3). Diferencias entre Telefonía IP y Telefonía tradicional. *Vertical Ibérica*. https://vertical-iberica.com/diferencias-entre-telefonia-ip-y-telefonia-tradicional/

LexGoApp. (s. f.). *Código Penal Federal (México)*. Recuperado 21 de enero de 2024, de https://lexgoapp.com/guias-legales/penal/codigo-penal-federal-mexico

Ley 25/2007 de 18 de octubre. Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. 8 de noviembre de 2007. BOE-A-2007-18243. https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243#:~:text=Esta%20Ley%20tiene%20por%20objeto,facultados%20siempre%20que%20les%20sean

Ley 34/2002 de 11 de julio. Servicios a la Sociedad de la Información y Comercio Electrónico. 12 de julio de 2002. BOE-A-2002-13758. https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

Ley 9/2014 de 9 de mayo. General de telecomunicaciones. 11 de mayo de 2014. BOE-A-2014-4950. https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

Ley Especial contra los Delitos Informáticos. 30 de octubre de 2001. Gaceta Oficial de la República Bolivariana de Venezuela, N° 37.313. https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, [L.F.P.D.P.P.P.], Nueva Ley, Diario Oficial de la Federación [D.O.F.], 5 de julio de 2010, (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal del Derecho de Autor [L.F.D.A.]. Reformada, Diario Oficial de la Federación [D.O.F.], 24 de diciembre de 1996, (México). https://www.ucol.mx/content/cms/13/file/federal/LEY_FED_DEL_DERECHO_DEL_AUTOR.pdf

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, [L.G.P.D.P.P.S.O.], Nueva Ley, Diario Oficial de la Federación [D.O.F.], 26 de enero de 2017. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996. Naciones Unidas. http://www.paginaspersonales.unam.mx/files/1719/Leccion_2_Ley_Modelo_sobre_comercio_electroni.pdf

Ley orgánica 3/2018 de 5 de diciembre. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. 6 de diciembre de 2018. BOE-A-2018-16673. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Limones, E. (2021, septiembre 17). *Protocolo de red: Qué es, tipos y características*. OpenWebinars.net. https://openwebinars.net/blog/protocolo-de-red-que-es-tipos-y-caracteristicas/

Limones, E. (2022, septiembre 23). *Análisis de vulnerabilidades informáticas*. OpenWebinars.net. https://openwebinars.net/blog/analisis-de-vulnerabilidades-informaticas/

López Barrientos, M. J., & Quezada Reyes, C. (2019). *Fundamentos de seguridad informática* (Segunda).

López Villalvazo., A. (2004a, junio 10). *Estándar 569*. *5*. https://www.revista.unam.mx/vol.5/num5/art28/art28-1b.htm

López Villalvazo., A. (2004b, junio 10). *Estándar 606. 5*. https://www.revista.unam.mx/vol.5/num5/art28/art28-1c.htm

Loredo González, J. A., & Ramírez Granados, A. (s. f.). *Delitos Informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo.* [Artículo., Universidad Autónoma de Nuevo León.]. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Lozada León, G. (2017, abril 4). *Soberanía popular e historia de la Ciudad de México.* Relatos e Historias en México. https://relatosehistorias.mx/nuestras-historias/soberania-popular-e-historia-de-la-ciudad-de-mexico

Lucana Mamani, U. (s. f.). *Criptografia*. Recuperado 14 de enero de 2024, de https://uninet.edu/6fevu/text/criptografia.htm

Malwarebytes. (s. f.). *Cryptojacking.* Recuperado 21 de enero de 2024, de https://es.malwarebytes.com/cryptojacking/

Marín, N. (2019, marzo 13). Covert Channel, exfiltración de información. *Sothis*. https://www.sothis.tech/covert-channel-exfiltracion-de-informacion/

Martín, A. (2020, agosto 13). *ReVoLTE: Una vulnerabilidad del VoLTE permite descifrar y escuchar llamadas 4G*. Hipertextual. http://hipertextual.com/2020/08/revolte

Martínez Alarcón, B. (2006). *La filosofía Hacking y Cracking.* [Monografía., Universidad Autónoma del Estado de Hidalgo.]. https://core.ac.uk/download/pdf/71450528.pdf

Martínez, J. L. (2018, junio 21). *¿Qué tipos de servidores hay? · Clasificación completa*. PRORED. https://www.prored.es/que-tipos-de-servidores-hay/

Martínez, V. (2021, diciembre 4). ¿Cómo surge el IFAI-INAI? *Cuestione.* https://cuestione.com/nacional/como-surge-ifai-inai-transparencia-corrupcion-estafa-maestra-casa-blanca-gobierno/

Martins, J. (2022, agosto 16). *Qué es un plan de contingencia y cómo crear uno en 8 pasos.* Asana. https://asana.com/es/resources/contingency-plan

Mateiu, M. (2018, julio 9). *Registradores de pulsaciones de teclas: Qué son, de dónde vienen y cómo eliminarlos*. AVG. https://www.avg.com/es/signal/keyloggers-what-they-are-where-they-come-from-and-how-to-remove-them

Maza Correa, J. P. (2023, diciembre 1). *El perfil del delincuente informático*. LawAndTrends. http://www.lawandtrends.com/noticias/tic/el-perfil-del-delincuente-informatico-1.html

Maza, A. (2021, enero 22). Del IFAI al Inai: La lucha por el derecho a saber. *El Sol de México.* https://www.elsoldemexico.com.mx/mexico/del-ifai-al-inai-la-lucha-por-el-derecho-a-saber-6274532.html

MDN Web Docs. (2023, noviembre 13). *World Wide Web*. Developer Mozilla. https://developer.mozilla.org/es/docs/Glossary/World_Wide_Web

Medina Velandia, L. N. (2017). *Criptografía y mecanismos de seguridad.* Fondo editorial Areandino. https://digitk.areandina.edu.co/bitstream/handle/areandina/1423/Criptograf%C3%ADa%20y%20mecanismos%20de%20seguridad.pdf?

Mendoza, M. Á. (2014a, julio 1). *Calculando pérdidas monetarias por riesgos de seguridad.* Welivesecurity. https://www.welivesecurity.com/la-es/2014/07/01/calculando-perdidas-monetarias-riesgos-seguridad/

Mendoza, M. Á. (2014b, agosto 18). *El ciclo de vida de las políticas de seguridad*. Welivesecurity. https://www.welivesecurity.com/la-es/2014/08/18/ciclo-de-vida-de-las-politicas-de-seguridad/

Mendoza, M. Á. (2015, marzo 23). *¿Evaluación de riesgos cualitativa o cuantitativa?* Welivesecurity. https://www.welivesecurity.com/la-es/2015/03/23/evaluacion-de-riesgos-cualitativa-o-cuantitativa/

Mieres, J. (2009). *Debilidades de seguridad comúnmente explotadas*. https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

MINTIC. (2016). *Elaboración de la política general de seguridad y privacidad de la información.* [Guía.]. https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Miralis, D. (s. f.). The Telecommunications (Interception and Access) Act 1979 (TIA Act). *NGM Lawyers*. Recuperado 25 de enero de 2024, de https://ngm.com.au/telecommunications-interception-and-access-act/

Moes, T. (2023, mayo). *¿Qué es un rootkit?* Software Lab. https://softwarelab.org/es/blog/que-es-un-rootkit/

Molinetti, S. (2020, enero 2). *La psicología detrás de los ciberdelitos*. Telefónica Tech. https://telefonicatech.com/blog/psicologia-ciberdelitos

Moreno López, J. A. (s. f.). *Defensa en profundidad*. http://polux.unipiloto.edu.co:8080/00001345.pdf

Moreno, A. (2021, noviembre 30). *Introducción a ataques activos y pasivos en seguridad informática*. Huawei. https://forum.huawei.com/enterprise/es/introducci%C3%B3n-a-ataques-

activos-y-pasivos-en-seguridad-inform%C3%A1tica/thread/667215571843956736-667212881550258176

Moreno, J. (2010, junio 21). *Evasión en IDS (I)*. Security Art Work. https://www.securityartwork.es/2010/06/21/evasion-en-ids-i/

Mundo a world of experts. (s. f.). *Agencias Gubernamentales Australianas.* Recuperado 25 de enero de 2024, de https://mundo.expert/es/Countries/Details/467?CountryId=55

Muñoz, F. (2017, mayo 14). *Qué es un troyano en informática*. Welivesecurity. https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/

Murphey, D. (2019, junio 27). A history of information security. *IFSEC Insider* | *Security and Fire News and Resources*. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Naciones Unidas. (2022, septiembre 27). *Historia de las Naciones Unidas.* https://unric.org/es/historia-de-las-naciones-unidas/

Naciones Unidas. (s. f.). *Sobre la CNUDMI.* Recuperado 25 de enero de 2024, de https://uncitral.un.org/es/about

National Association of Criminal Defense Lawyers. (s. f.). *Computer Fraud and Abuse Act (CFAA).* NACDL. Recuperado 25 de enero de 2024, de https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

NETSCOUT. (s. f.-a). *What is a Slowloris Attack?* Recuperado 21 de enero de 2024, de https://www.netscout.com/what-is-ddos/slowloris-attacks

NETSCOUT. (s. f.-b). *What is packet sniffing?* Recuperado 19 de enero de 2024, de https://www.netscout.com/what-is/sniffer

Netskope. (s. f.). *¿Qué es un Cyber Security Kill Chain?* Recuperado 19 de enero de 2024, de https://www.netskope.com/es/security-defined/cyber-security-kill-chain

NIC Argentina. (2017, diciembre). *ARPANET: El origen de Internet*. http://nic.ar/es/enterate/novedades/arpanet-el-origen-de-internet

NIC Argentina. (2018, junio). *¿Cómo funciona el DNS?* http://nic.ar/es/novedades/noticias/como-funciona-el-dns

NIST. (2021, febrero 25). *Secure Software Development Framework.* https://csrc.nist.gov/Projects/ssdf

NMAP. (s. f.). *Técnicas de sondeo de puertos*. Recuperado 19 de enero de 2024, de https://nmap.org/man/es/man-port-scanning-techniques.html

Normas ISO. (s. f.). *ISO 27001 - Seguridad de la información: Norma ISO IEC 27001/27002*. Recuperado 13 de enero de 2024, de https://www.normas-iso.com/iso-27001/

Normativa y Regulación Informática. (2015, febrero 7). *Ética y Deontología Informática: Conceptos Básicos.* https://nrioly.wordpress.com/bloque-i-1/conceptos/

Norton. (2018a, agosto 8). *¿Qué es la ingeniería social?* https://mx.norton.com/blog/emerging-threats/what-is-social-engineering

Norton. (2018b, agosto 8). *¿Qué es un troyano?* https://mx.norton.com/blog/malware/what-is-a-trojan

Notes De Seguretat. (2022, abril 11). *Proceso de reforma del marco de vigilancia electrónica en Australia.* https://notesdeseguretat.blog.gencat.cat/2022/04/11/proceso-de-reforma-del-marco-de-vigilancia-electronica-en-australia/

Noticias ONU. (2019, mayo 7). *Los desechos electrónicos, una oportunidad de oro para el trabajo decente.* Naciones Unidas. https://news.un.org/es/story/2019/04/1455621

Notimex. (2015, mayo 5). Ifai cambia de nombre; se transforma en Inai. *El Economista*. https://www.eleconomista.com.mx/politica/Ifai-cambia-de-nombre-se-transforma-en-Inai-20150505-0198.html

Ochoa Serafín, M. (2023, diciembre 1). Delitos Informáticos en México y por qué los mexicanos estamos en peligro. *IT Masters Mag*. https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

Odón de Buen, C. N. para el U. E. de la. (2017, junio 20). *Sobre la importancia de los trabajos de la Comisión Electrotécnica Internacional (IEC)*. gob.mx. http://www.gob.mx/conuee/articulos/sobre-la-importancia-de-los-trabajos-de-la-comision-electrotecnica-internacional-iec

Olmos Guarneros, F. (2022, diciembre 30). Los daños a la ciberseguridad crecen 144% cada año y esto se espera para 2023. *Expansión*. https://expansion.mx/tecnologia/2022/12/30/que-espera-2023-en-ciberataques

Oracle. (s. f.). *¿Qué es una base de datos?* Recuperado 19 de enero de 2024, de https://www.oracle.com/mx/database/what-is-database/

Organización Mundial de la Propiedad Intelectual. (s. f.). *Derecho de autor*. Recuperado 21 de enero de 2024, de https://www.wipo.int/copyright/es/index.html

Ortíz Anderson, C. (s. f.). *La importancia de un plan de contingencia.* Recuperado 21 de enero de 2024, de https://www.forodeseguridad.com/artic/discipl/4132.htm

Otake, L. (2019, octubre 21). COBIT 2019. *AudiConsulti*. https://www.audiconsulti.com/glosario/que-es-cobit-2019/

OWASP.org. (s. f.). *OWASP SAMM.* Recuperado 19 de enero de 2024, de https://owasp.org/www-project-samm/

Paessler. (s. f.). *¿Qué es la detección de paquetes?* Recuperado 19 de enero de 2024, de https://www.paessler.com/es/it-explained/packet-sniffing

Panda Security. (2023, enero 18). ¿Qué es un hacker de sombrero blanco? *Panda Security Mediacenter*. https://www.pandasecurity.com/es/mediacenter/hacker-sombrero-blanco/

Paz, Á. (2008, agosto 28). Enmascarar sistema para evitar OS Fingerprinting. *GURÚ DE LA INFORMÁTICA*. https://gurudelainformatica.es/enmascarar-sistema-para-evitar-os-fingerprinting

PCHARDWAREPRO. (2023, noviembre 8). *¿Qué es Metasploit y cómo utilizarlo correctamente?* https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente/

Pearson. (2013, febrero 4). *CISSP Exam Cram: Security Architecture and Models*. Pearson IT Certification. https://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=5

Pedroza, S. (2021, septiembre 28). Phreaker. *Muy Tecnológicos*. https://muytecnologicos.com/diccionario-tecnologico/phreaker-que-es

Pérez-Roca Fernández, J. Á., & Pereira Suárez, J. A. (s. f.). *Firewalls*. http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf

Personal Information Protection and Electronic Documents Act. (2019, 21 junio). Justice Laws Website. https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html

Pirani. (s. f.-a). *Guía para hacer una Política de Seguridad de la Información.* Recuperado 21 de enero de 2024, de https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion

Pirani. (s. f.-b). *Guía para realizar la evaluación de riesgos.* Recuperado 21 de enero de 2024, de https://www.piranirisk.com/es/academia/especiales/guia-para-realizar-la-evaluacion-del-riesgo

PlataformaPYME. (s. f.). *La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI, (UNCITRAL).* Recuperado 25 de enero de 2024, de https://plataformapyme.es/es-es/Internacional/OtrasInstituciones/Paginas/CNUDMI.aspx

Platzi. (2019). *Arquitectura de metasploit*. https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

Polanco, M. (2019, febrero 10). Ciclo de vida de los ataques avanzados. *Magazcitum*. https://www.magazcitum.com.mx/index.php/archivos/3034

Ponce, J. L. (2023, marzo 11). ¿Qué es la Ley de Protección de datos en México y cuál es su importancia? *Ikusi MX*. https://www.ikusi.com/mx/blog/ley-de-proteccion-de-datos-en-mexico/

Portal Administración electrónica. (s. f.). *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* PAe. Recuperado 21 de enero de 2024, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Presidencia de la República. (2013, abril 23). *Conoce más sobre los Derechos de Autor*. gob.mx. http://www.gob.mx/epn/articulos/conoce-mas-sobre-los-derechos-de-autor

PricewaterhouseCoopers. (s. f.). *Un panorama de la ciberseguridad en México*. Recuperado 13 de enero de 2024, de https://www.pwc.com/mx/es/ciberseguridad/digital-trust.html

Proofpoint. (2021, octubre 19). *¿Qué es el vishing?* https://www.proofpoint.com/es/threat-reference/vishing

Proofpoint. (2022, junio 14). *¿Qué es el cryptojacking?* https://www.proofpoint.com/es/threat-reference/cryptojacking

Ptolomeo UNAM. (s. f.-a). *Capitulo 2. Amenazas y vulnerabilidades de la seguridad informático*. http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A5.pdf?sequence=5

Ptolomeo UNAM. (s. f.-b). *Seguridad Informática*. http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/250/A5.pdf?sequence=5&isAllowed=y

Ralco Networks. (2020, noviembre 23). *Conoce los Tipos de Ciberataques y las Mejores Prácticas* -. https://www.ralco-networks.com/conoce-los-tipos-de-ciberataques-y-las-mejores-practicas/

Ramírez González, A. E. (s. f.). *Monitor de Enlaces IP.* [Tesis Profesional, Universidad Tecnológica Mixteca]. Recuperado 20 de enero de 2024, de https://1library.co/article/el-modo-promiscuo-pdf.dy40m55z

Redes Inalambricas. (s. f.). *¿Qué es una Red Inalámbrica?* redesinalambricas.es. Recuperado 19 de enero de 2024, de https://www.redesinalambricas.es/

Rentería Echeverry, F. A. (s. f.). *Inicio y Evolución de la Seguridad Informática en el Mundo* [Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00001532.pdf

Responsaibilidad Social Empresarial y Sustentabilidad. (2022, septiembre 16). *Ética: Qué es, Definición, Origen, Tipos y Ejemplos.* https://responsabilidadsocial.net/etica-que-es-definicion-origen-tipos-y-ejemplos/

Revista Fortuna. (2022, octubre 26). *La ruta hacia la Ley de Ciberseguridad en México*. https://revistafortuna.com.mx/2022/10/26/la-ruta-hacia-la-ley-de-ciberseguridad-en-mexico/

Revista Seguridad 360. (2021, diciembre 23). *Conozca los tipos de delitos informáticos más frecuentes.* https://revistaseguridad360.com/destacados/tipos-de-delitos-informaticos/

Reyes Castro, J. E., & Porras Garzón, L. O. (s. f.). *Riesgos Residuales.* [Artículo., Universidad Piloto de Colombia.]. http://polux.unipiloto.edu.co:8080/00001168.pdf

Ribas, E. (2022, mayo 17). Cryptojacking: Qué es, cómo funciona y cómo evitarlo. *IEBS.* https://www.iebschool.com/blog/que-es-cryptojacking-finanzas/

Riffo Gitiérrez, M. A. (2009). *Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad.* [Tesis, Universidad Austral de Chile]. http://cybertesis.uach.cl/tesis/uach/2009/bmfcir564v/doc/bmfcir564v.pdf

Rivero, M. (2009, marzo 19). *¿Qué son los Rootkits?* InfoSpyware. https://www.infospyware.com/articulos/que-son-los-rootkits/

Rodriguez, E. (2020, marzo 10). *¿Qué es el plan de contingencia de una empresa?* [Text]. Ayse Lucus. https://www.ayselucus.es/noticia/%C2%BFqu%C3%A9-es-el-plan-de-contingencia-de-una-empresa

Rojas Armandi, V. (s. f.). *La Ley Modelo de Comercio Electrónico de la Comisión de Naciones Unidas de Derecho Mercantil Internacional.* https://revistas.ibero.mx/juridica/articulos_pdf/861682.pdf

Rojo García, E. (2022, marzo 1). Los datos personales y la Ley Patriota de Estados Unidos. *Abogacía*. https://www.revistaabogacia.com/los-datos-personales-y-la-ley-patriota-de-estados-unidos/

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1.ª ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

Romero Pérez, J. U., Ramírez Torres, M. G., Arreola Núñez, M. L., Hurtado Torres, R., & Suárez Ramírez, M. (2021, abril 24). *La Gestión de riesgos ¿para qué?* impuestos.info. https://impuestos.info/la-gestion-de-riesgos-para-que/

Romero Vanegas, A. Y. (s. f.). *Pentesting, ¿Porque es importante para las empresas?* [Artículo., Universidad Piloto de Colombia.]. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

Ropero, A. (2015, junio 30). *Más de 70.000 vulnerabilidades*. Una al Día. https://unaaldia.hispasec.com/2015/06/mas-de-70-000-vulnerabilidades.html

Rubio Díaz, R. (2019, febrero 26). 10 Beneficios de un Sistema de Cableado Estructurado. *Unitel - Soluciones e infraestructuras Tecnológicas*. https://unitel-tc.com/10-beneficios-de-un-sistema-de-cableado-estructurado/

Ruge Pinzón, J. N. (2011). *Metodología para identificación y valoración de riesgos y salvaguardad en una mesa de ayuda tecnológica.* [Trabajo de grado., Universidad Piloto de Colombia.]. http://polux.unipiloto.edu.co:8080/00000744.pdf

Sandoval Castellanos, E. J. (s. f.). *Ingeniería Social: Corrompiendo la mente humana.* Recuperado 19 de enero de 2024, de https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Santander Universidades. (2022, enero 13). *Misión, visión y valores de una empresa: Qué son y cómo definirlos.* https://www.santanderopenacademy.com/es/blog/mision-vision-y-valores.html

SayNet. (s. f.). *¿Qué es un análisis de vulnerabilidades?* Recuperado 21 de enero de 2024, de https://saynet.com.mx/que-es-un-analisis-de-vulnerabilidades/

Secretaría de la Defensa Nacional. (s. f.). *28 de diciembre de 1836, España reconoce oficialmente la independencia de México.* gob.mx. Recuperado 21 de enero de 2024, de http://www.gob.mx/sedena/documentos/28-de-diciembre-de-1836-espana-reconoce-oficialmente-la-independencia-de-mexico?state=published

Sicma21, P. (2021, junio 14). *Mantenimiento correctivo: Todo lo que necesitas saber.* https://www.sicma21.com/mantenimiento-correctivo-que-es-y-como-funciona/

Silva, N., & Espina, J. (2006). *Ética Informática en la Sociedad de la Información. 11*(36), 559-579.

SNK, S. (2018, octubre 21). La Importancia De La Ética En La Actualidad. *Medium*. https://medium.com/@jesushbk97/la-importancia-de-la-%C3%A9tica-en-la-actualidad-e23dfe8d92c6

Software DELSOL. (2020, diciembre 9). *Deontología.* https://www.sdelsol.com/glosario/deontologia/

Sosa Barrientos, T. Y., Chacón Morales, K. M., Cordón y Cordón, B. G., De León Enamorado, E. A., Cruz Vargas, L. A., Leonardo Ismatul, M. N., & Orellana Ortiz, J. A. (2015, febrero 28). Ética Informática en el mundo moderno. *Temarios Auditoria B2*. https://auditoresprimeringreso.wordpress.com/etica-informatica-en-el-mundo-moderno/

Spiegato. (2021a, julio 25). *¿Qué es el modo promiscuo?* https://spiegato.com/es/que-es-el-modo-promiscuo

Spiegato. (2021b, julio 25). *¿Qué es la Ley de Privacidad de las Comunicaciones Electrónicas?* https://spiegato.com/es/que-es-la-ley-de-privacidad-de-las-comunicaciones-electronicas

Surveillance Devices Act 2007. (2022, 16 mayo). NSW legislation. https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-064#:~:text=(1)%20A%20person%20must%20not,a%20listening%20device%2C%20an%20optical

Tarazona T, C. H. (1969). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, *28*(84), Article 84.

Tavella, F. (2021, marzo 4). *Qué es un keylogger: Una herramienta para espiar*. Welivesecurity. https://www.welivesecurity.com/la-es/2021/03/04/que-es-keylogger-herramienta-para-espiar/

Tech. (s. f.). *¿Qué es Metasploit? Guía para principiantes.* Recuperado 20 de enero de 2024, de https://tech-es.netlify.app/articles/es528578/index.html

Tecnocosas. (2018, octubre 26). *Ataques más comunes a las redes inalámbricas.* https://www.tecnocosas.es/ataques-mas-comunes-a-las-redes-inalambricas/

Teoyotl Calderón, Y. (2013). *Seguridad en las redes inalambricas.* [Tesis., Universidad Nacional Autónoma de México.]. http://132.248.9.195/ptd2013/febrero/0689006/0689006.pdf

Thales. (s. f.). *Cumplimiento de PIPEDA.* Recuperado 25 de enero de 2024, de https://cpl.thalesgroup.com/es/compliance/americas/pipeda-compliance

TIC Portal. (2023, diciembre 7). *¿Qué es un servidor, cómo funciona y qué tipos hay?* https://www.ticportal.es/glosario-tic/servidores

Toro, R. (2015, marzo 16). ISO 27001: El método MAGERIT. *Grupo ESGinnova.* https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Toro, R. (2017, febrero 23). ¿Cómo realizar un inventario de activos de información? *Grupo ESGinnova*. https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Tovar, D. (2022, mayo 20). ¿Cómo comunicar los cambios de política a los empleados? *Innatos.* https://innatos.com.mx/comunicar-cambios-politica-empleados/

Trend Micro. (s. f.). *¿Cuáles son los diferentes tipos de phishing?* Recuperado 14 de enero de 2024, de https://www.trendmicro.com/es_es/what-is/phishing/types-of-phishing.html

Triana Tacuma, E. (2017, diciembre). *Ética Informática. 12*(3). http://www.spentamexico.org/v12-n3/A17.12(3)272-279.pdf

Trujillo, E. (2020, agosto 3). *Código penal*. Economipedia. https://economipedia.com/definiciones/codigo-penal.html

Tyas Tunggal, A. (2023, abril 20). *What is PIPEDA (Personal Information Protection and Electronic Documents Act)?* https://www.upguard.com/blog/pipeda

Ugarte, I. (2022, octubre 26). El daño a la reputación de una compañía, causado por un ciberataque, puede ser irreparable y definitivo. *Secure&IT*. https://www.secureit.es/el-dano-a-

la-reputacion-de-una-compania-causado-por-un-ciberataque-puede-ser-irreparable-y-definitivo/

UNAM. (s. f.). *Diseño de una VPN*. http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/250/A7.pdf?sequence=7&isAllowed=y

UNAM. (s. f.-a). *Negación de servicio.* Recuperado 21 de enero de 2024, de https://revista.seguridad.unam.mx/category/tipo-de-articulo/negaci%C3%B3n-de-servicio

UNAM. (s. f.-b). *Tema 3. Análisis de riesgo.* http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/203/A6.pdf?sequence=6&isAllowed=y

UNIR México. (2022, abril 11). *¿Qué es la misión y visión de una empresa?: 6 ejemplos de grandes compañías.* https://mexico.unir.net/mba/noticias/mision-vision-empresa/

United States Code [USC], Título 18, Sección 1030 – Fraud and related activity in connection with computers, (USA). https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)

United States Code [USC], Título 18, Secciones 2510 a 2523 – Wire and Electronic Communications Interception and Interception of Oral Communications, (USA).

United States Code [USC], Título 18, Secciones 2701 a 2713 – Stored Wire and Electronic Communications and Transactional Records Access (USA).

United States Code [USC], Título 18, Secciones 3121 a 3127 – Pen Registers and Trap and Trace Devices, (USA).

United States Code [USC]. Título 18, Sección 1029 – Fraud and related activity in connection with access devices, (USA). https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1029)&num=0&edition=prelim

Unitel. (2013, septiembre 24). *Normas sobre Cableado Estructurado.* https://unitel-tc.com/normas-sobre-cableado-estructurado/

Universidad de Jaén. (s. f.). *Nombres de Dominio (DNS)*. Recuperado 19 de enero de 2024, de https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns

Universidad de los Andes. (s. f.). *¿Qué es ACM?* Recuperado 26 de enero de 2024, de https://acm.uniandes.edu.co/?page_id=13

Universidad Internacional Valencia. (2022, abril 25). *Los tipos de software y sus diferencias que debemos conocer*. VIU España. https://www.universidadviu.com/es/actualidad/nuestros-expertos/los-tipos-de-software-y-sus-diferencias-que-debemos-conocer

Universidad Oberta de Catalunya. (2017, abril 26). *La UOC y la URV desarrollan un sistema que oculta automáticamente la información confidencial de documentos.* https://www.uoc.edu/es/news/2017/100-informacion-confidencial

Universidad Oberta de Catalunya. (s. f.). *Los activos de la organización*. Recuperado 21 de enero de 2024, de https://cv.uoc.edu/UOC/a/moduls/90/90_331/web/main/m1/v1_1_4.html

Universidad Veracruzana. (2016, abril 1). *Conocimientos generales: ¿Qué es el malware y cómo se clasifica?* https://www.uv.mx/infosegura/general/conocimientos_virus-2/

UPAEP. (s. f.). *¿Qué es el Derecho de Autor?* Recuperado 21 de enero de 2024, de https://investigacion.upaep.mx/index.php/derecho-de-autor

USAGov. (2023, diciembre 12). *Robo de identidad.* https://www.usa.gov/es/robo-identidad

USS. (2019, enero 12). Tipos de Ataques DNS: ¿Cuántos Existen y Cómo Evitarlos? *Blog de Seguridad para Empresas*. https://uss.com.ar/corporativo/tipos-ataques-dns-cuantos-existen-evitarlos/

Valenzuela González, C. (2022, abril 14). *Estos son los 4 ataques más comunes que atentan contra tus contraseñas y cómo protegerte*. Computer Hoy. https://computerhoy.com/noticias/tecnologia/estos-son-4-ataques-comunes-atentan-contrasenas-como-protegerte-1045157

Valenzuela, L. (2021, enero 6). La función constitucional del INAI es intransferible e irrenunciable. *Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales*. https://idaip.org.mx/sitio/2021/01/06/la-funcion-constitucional-del-inai-es-intransferible-e-irrenunciable/

Vaquero, C. P. (2020, febrero 7). Anécdotas y curiosidades jurídicas. *Anécdotas y curiosidades jurídicas | iustopía*. https://archivodeinalbis.blogspot.com/2020/02/el-codigo-de-los-estados-unidos-uscode.html

Vasquez, M. D. (2016). *Técnicas Anti-Forenses Informáticas.* [Trabajo Final Integrador., Universidad Nacional de Córdoba.]. https://www.famaf.unc.edu.ar/documents/1305/1-Miguel_Vasquez.pdf

Velasco Bautista, C., López Hernández, J., Nakano Miyatake, M., & Pérez Meana, H. (2007). *Esteganografía en una imágen digital en el dominio DCT. 11.*(4.). https://www.redalyc.org/pdf/614/61411403.pdf

Vélez Martínez, C. (s. f.). *Passwords*. Recuperado 20 de enero de 2024, de https://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/passwords.aspx

Vélez Martínez, C. (s. f.). *Hackers*. Recuperado 14 de enero de 2024, de https://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx

Venfort. (2019, mayo 30). *Aspectos de la Ley Especial contra Delitos Informáticos en Venezuela.* Venfort. https://venfort.com/es/ley-especial-contra-delitos-informaticos/

Verdejo Álvarez, G. (s. f.). *Denegación de servicio: DOS/DDOS.* Recuperado 21 de enero de 2024, de https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf

Vidal Casero, M. del C. (s. f.). *Información sobre códigos deontológicos y directrices sobre ética en internet. 5*(4). https://www.bioeticacs.org/iceb/seleccion_temas/deontologia/CODIGOS_DEONTOLOGICOS.pdf

VIEWNEXT. (2020, septiembre 17). *Técnicas de ingeniería social*. https://www.viewnext.com/tecnicas-de-ingenieria-social/

Vilches Abogados. (2018, febrero 8). *Acceso ilícito a sistemas informáticos.* https://blog.hernandez-vilches.com/ciberdelitos/intrusion-informatica-acceso-ilicito/

Weis, O. (2021, junio 7). *Qué es Ethernet y Cómo Funciona.* USB Network Gate. https://www.net-usb.com/es/usb-over-ethernet-system/what-is-ethernet/

WP Engine. (2024, enero 1). *Comprehensive Passwords List: Analysis & Insights from 10 Million Entries*. https://wpengine.com/resources/passwords-unmasked-infographic/

Wright, G. (s. f.). *Dumpster diving*. Security. Recuperado 19 de enero de 2024, de https://www.techtarget.com/searchsecurity/definition/dumpster-diving

Zambrano, N. (2020, noviembre 17). Ataque de OS Finger Printing ¿Qué es, cuáles son sus tipos y cómo evitarlos y protegernos para una mayor seguridad informática? *Internet Paso a Paso*. https://internetpasoapaso.com/ataque-os-finger-printing/