UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

PROGRAMA DE MAESTRIA Y DOCTORADO
EN INGENIERIA

FACULTAD DE INGENIERIA

IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD EN EL SISTEMA DE GESTIÓN ACADÉMICO/ADMINISTRATIVA DEL POSGRADO DE LA FACULTAD DE ECONOMÍA, UNAM

TESIS
QUE PARA OPTAR POR EL GRADO DE
MAESTRA EN INGENIERÍA
INGENIERÍA ELÉCTRICA – TELECOMUNICACIONES

P R E S E N T A :
LAURA LÁZARO RODRÍGUEZ

DIRECTOR DE TESIS
DR. FRANCISCO J. GARCÍA UGALDE

CODIRECTOR
M. EN I. JORGE VALERIANO ASSEM

MEXICO, D.F. 2009

JURADO ASIGNADO:

Presidente:	***Dr. Víctor Rangel Licea***
Secretario:	***M. en C. María Guadalupe Elena Ibargüengoitia González***
Vocal:	***Dr. Francisco García Ugalde***
Primer suplente:	***Dra. Hanna Okthaba***
Segundo Suplente:	***M. en I. Jorge Valeriano Assem***

DIRECTOR DE TESIS:

Dr. Francisco García Ugalde

CO- DIRECTOR DE TESIS:

M. en I. Jorge Valeriano Assem

A la **Universidad Nacional Autónoma de México** y a la Facultad de Ingeniería – División de Estudios de Posgrado por permitirme ser parte de ella, por los conocimientos adquiridos y por la apertura al conocimiento.

A la Facultad de Economía - División de Estudios de Posgrado, por permitirme realizar este trabajo, por darme la oportunidad de aplicar el conocimiento y experiencia adquiridos, y permitirme retomar el vuelo.

A mi director y codirector de tesis, por su apoyo en la culminación de esta meta en mi carrera profesional. Un agradecimiento especial al M. en I. Alejandro Velázquez Mena, por el tiempo y aportaciones a este trabajo.

Al jurado, por todas y cada una de las recomendaciones realizadas ya que me ayudaron a tener una visión más completa de lo que es la investigación, por el tiempo y las valiosas sugerencias para enriquecer este trabajo

Al personal del Centro de Informática de la Facultad de Economía, amigos y compañeros: Pilar Valeriano, Omar Sánchez, Arturo López, Jesús Garrido.

Al personal de la División de Estudios de Posgrado, por la información proporcionada y el apoyo durante este proceso: Leticia Saldaña, Ana Mercedes Morales, Alejandra Contreras, Alicia Hernández, Leticia García y Juanita Romero.

A mi hija Karen, pequeñita hermosa, por ser el mejor regalo en mi vida, por tus palabras de aliento, por tu sonrisa y por tus invitaciones a jugar, dándome un espacio de relajamiento en todo este proceso.

Gracias mi amor

A mi familia por todo el apoyo recibido en todas y cada una de las etapas de mi vida, en especial a mi muy querida hermana Yola.

Infinitamente gracias, querida hermana

Un agradecimiento especial a todas aquellas personas con quienes he compartido tiempo y espacio, ya que de todas ellas he aprendido; en especial a Janete Mejía, José Juan Pérez, Felipe Fernández, Pilar Valeriano, Omar Sánchez y Alejandro Talavera por su apoyo, porque siempre tuvieron una palabra de aliento, una visión distinta a la mía, una respuesta acertada o un consejo especial que me han ayudado a crecer como profesional y como ser humano.

Gracias por formar parte de mi historia

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El avance tecnológico en las últimas décadas permite el uso de herramientas de cómputo que ayudan a la automatización de tareas y almacenamiento electrónico de la información, sin embargo esto también tiene sus inconvenientes, los cuales pueden llegar a representar serias amenazas en el funcionamiento de parte o toda una organización.

Actualmente casi todo tipo de organización cuenta con información propia y en ocasiones compartida, por lo que se debe contar con mecanismos de seguridad a través de los cuales se proteja, controle y verifique la información con la que se opera; el no contar con estos mecanismos expone a la información a diversas vulnerabilidades que, ya sea realizadas sólo por curiosidad o con premeditación, pueden llegar a dañar a la organización a diversos niveles.

Una de las amenazas asociadas al uso de infraestructuras de comunicaciones es la posibilidad de accesos no autorizados o el uso inadecuado de los recursos informáticos; estas amenazas son una de las principales razones para pensar en el aseguramiento no sólo de la infraestructura de comunicaciones de una organización, sino también de las áreas físicas que resguardan la información, ya que ésta al ser uno de los recursos más preciados para cualquier organización debe ser asegurada de manera específica a fin de preservar su integridad, confiabilidad y disponibilidad.

Antecedentes

La Facultad de Economía inició en el año 2002 un proyecto de modernización que dotara de infraestructura de comunicaciones a las diversas áreas que la integran; este esfuerzo generó el dotar con equipo de cómputo a las áreas académicas en primer lugar para posteriormente cubrir las áreas administrativas.

Actualmente la situación ha cambiado, ya que la adecuación realizada no contempló la capacitación periódica del personal que utiliza el equipo, la protección individual de los equipos, el mantenimiento de los mismos y, sobre todo, la revisión de su utilización dentro de las instalaciones de la Facultad.

Otro factor que ha surgido es el crecimiento de la interrelación de académicos con pares de otras instituciones y el incremento en la investigación que se realiza, por lo que se requiere de la creación de un plan de seguridad que subsane las deficiencias de la infraestructura actual.

La División de Estudios de Posgrado de la Facultad de Economía (DEP-FE) apoyando este proceso de modernización inició en el 2005 un esfuerzo de automatización de procesos para el registro y gestión de información académico-administrativa asociada con la productividad de la planta académica, el seguimiento de alumnos inscritos en los programas académicos de maestría y doctorado, así como de las actividades administrativas propias de la Jefatura de esta División.

Definición del Problema

Cualquier sistema de comunicaciones conlleva diversos riesgos operacionales que pueden tener su origen en diversas fuentes: errores en la entrada de datos, amenazas internas y/o externas, la propia infraestructura de red, la ingeniería social e incluso desastres naturales.

La seguridad establecida en la División de Estudios de Posgrado de la Facultad de Economía comienza a ser insuficiente para la infraestructura actual de comunicaciones y operaciones que se realizan, para los sistemas de información con que se cuenta así como para el crecimiento que se está dando en cuanto a proyectos de investigación e interrelación con investigadores de otras entidades académicas nacionales e internacionales.

La información sensible y/o crítica de la DEP-FE al ser procesada, almacenada, impresa, eliminada y transmitida a través de diversos medios dentro y fuera de la organización debe ser protegida, por lo que cuanto antes se adopten las medidas preventivas y correctivas para evitar y/o disminuir las vulnerabilidades de seguridad, éstas representarán un menor costo y serán más efectivas con la consecuente minimización del riesgo o pérdida.

Objetivo y metodología

El presente trabajo de tesis tiene como objetivo la implementación de mecanismos de seguridad en los sistemas de información académico-administrativos de la División de Estudios de Posgrado de la Facultad de Economía que protejan la información con la que se trabaja de manera cotidiana.

Aún cuando la seguridad de la información puede lograrse por medios técnicos esto llega a ser limitado, por lo que el aseguramiento debe ser respaldado por una gestión y serie de procedimientos exprofeso para cada elemento a proteger.

Debido a esto, también se definirá una Política de Seguridad de la Información que indique de manera clara y precisa los mecanismos a utilizar en la protección de la información que se genera, transmite y almacena en las diversas áreas académico-administrativas de la DEP-FE mediante los sistemas de información implementados a la fecha.

Esta política de seguridad debe incluir las contramedidas necesarias para evitar se produzca un evento negativo, y evitar con ello las pérdidas de tiempo, recursos, económicos y/o de imagen; éste programa de seguridad debe incluir los controles a implementar como resultado del análisis y evaluación de riesgos realizados.

Para realizar el presente trabajo se utilizó como metodología de desarrollo la norma ISO/IEC 17799, la cual integra aspectos relacionados con las tecnologías de la información y aspectos administrativos tales como dirección, supervisión y control de recursos de las organizaciones a niveles tácticos, estratégicos y operativos, constituyendo así un marco de seguridad a todos los niveles dentro de la organización.

Contribuciones

Dentro de las contribuciones que genera el presente trabajo se encuentran:

- *Concientizar* a todo el personal de la DEP-FE, desde directivos hasta personal operativo, de la necesidad de gestionar la seguridad de la información, ya que con ello se obtendrán beneficios que redundarán en un mejor manejo de la información.
- *Evidenciar la necesidad de contar con mecanismos de protección*, tanto para la infraestructura física como de comunicaciones.
- *Generar y aplicar una política de seguridad de la información* que indique de manera puntual lo que está permitido y lo que está prohibido realizar con la información generada, transferida y almacenada por los sistemas y procesos de operación de la DEP-FE.
- *Documentar* los procesos críticos de operación indicando responsable, involucrados, límites operacionales y periodicidad de ejecución.
- *Generar respaldos de información* de manera periódica.

Los puntos mencionados ayudarán en una primera etapa a que la DEP-FE cuente con la documentación correspondiente a los procesos críticos de operación. De igual manera, al centrarse en los procesos y no en las personas se está evitando una dependencia que llega a ser perjudicial para cualquier organización.

El desarrollo de este trabajo también servirá como marco de referencia para aquellas organizaciones o entidades que deseen conocer e implementar controles de seguridad de la información ya sea en los sistemas de información o en la infraestructura con que cuente.

Estructura de la Tesis

En el presente trabajo se abordan cuestiones de seguridad asociadas al entorno físico de la información, a la infraestructura de comunicaciones, y a los procesos de registro y almacenamiento de información; para ello se ha desarrollado un Sistema de Gestión de Seguridad de la Información (SGSI), el cual cubre aspectos tanto físicos como lógicos de la información: registro, proceso, transferencia y almacenamiento.

En el Capítulo 1 se presenta el marco teórico de la seguridad informática, su evolución, y los organismos internacionales enfocados a normalizar actividades y procesos de seguridad asociados tanto a la propia evolución tecnológica como a casos de error o negligencia humana. Se presentan las normas y estándares de seguridad que han desarrollado estos organismos con la finalidad de proteger la información y la infraestructura asociada, mismos que son revisados periódicamente para su validación y adaptación a nuevas formas de ataque y así prevenir riesgos operacionales y humanos.

En el Capítulo 2 se aborda la inseguridad de la infraestructura de comunicaciones a la que puede estar expuesta cualquier organización, indicando las amenazas y vulnerabilidades genéricas que afectan el buen desempeño de la red, siendo el factor humano uno de los más involucrados.

Estas amenazas y vulnerabilidades revelan que en cuestión de infraestructura de comunicaciones lo crítico ya no sólo es el ancho de banda, la protección perimetral y el uso de aplicaciones, sino también la seguridad de los contenidos que viajan por la red aunado a la identidad de los usuarios que generan y acceden a esa información; es por ello que se presentan algunos métodos y herramientas de protección que si bien en algunos casos no eliminan la amenaza, sí la minimizan para que cause el menor daño posible.

En el Capítulo 3 se abordan algunos métodos de protección y prevención, entre los que se encuentran la definición e implementación de Políticas de Seguridad de la Información (PSI), los modelos de seguridad, los planes y procedimientos de contingencia, y otros sistemas y mecanismos de protección, los cuales pueden ser implementados en cualquier infraestructura de comunicaciones que se quiera proteger.

Se abordan los aspectos a tomar en cuenta durante la formulación y el ciclo de vida de una PSI ya que éstos dependerán del nivel de seguridad con que cuenta la entidad y al cual se desea llegar. Una actividad importante asociada a la implementación de una política de seguridad es la generación de planes y procedimientos de contingencia, los cuales permiten a la organización continuar operando de manera similar a como lo haría hasta antes de algún ataque o imprevisto, y más aún, indican la forma en que se debe reaccionar ante un ataque, la resolución del problema y la prevención del mismo.

En el Capítulo 4 se presenta el desarrollo e implementación de un Sistema de Gestión de Seguridad de la Información para la División de Estudios de Posgrado de la Facultad de Economía (DEP-FE).

En primer lugar se proporciona un panorama general de las actividades que se realizan en esta División, el personal que la conforma y la infraestructura física y de comunicaciones con que cuenta, realizando un análisis de la seguridad actual.

Posteriormente se presenta el desarrollo del SGSI apoyados en la norma internacional ISO/IEC 17799. Se seleccionó esta norma de seguridad ya que a la fecha es la única que cubre aspectos no sólo relacionados con las Tecnologías de la Información (TI), sino que también abarca aquellos que pueden ser afectados en su funcionalidad y/o que son parte importante en los procesos de generación y resguardo de información dentro de cualquier entidad.

En la parte final de este capítulo se aborda el tema de Plan de Recuperación al Desastre (DRP, por sus siglas en inglés), el cual es un componente importante en cualquier SGSI ya que se deben cubrir todas las posibilidades de ataque o interrupción a las actividades operativas de la DEP-FE y contar con una solución inmediata a cualquiera de éstas.

En el Capítulo 5 se presenta los resultados de este proyecto, donde la Política de Seguridad de la Información es uno de los principales ya que es el soporte para una buena administración y resguardo de la información. Presenta el objetivo, vigencia, roles y responsabilidades en cuanto al manejo de la seguridad de la información, clasificación de la información y las políticas en sí mismas.

Para realizar este SGSI y su implementación, se aplicó un cuestionario con los 127 controles contemplados por la norma ISO/IEC 17799, el cual proporciona una idea del estado actual de la seguridad en la entidad de estudio; este cuestionario se presenta en el Anexo 1.

En el Anexo 2 se hace una primera aproximación a los controles que originalmente fueron seleccionados para su desarrollo y aplicación así como la propuesta de solución para cada uno de ellos. Estos controles se enfocaron a tres aspectos generales: Gestión de operaciones y comunicaciones, Control de accesos y Desarrollo y mantenimientos de sistemas de información.

Finalmente, en el Anexo 3 se presentan los procedimientos operativos que deben seguirse a fin de cubrir aspectos esenciales antes, durante y después de una contingencia. Los procesos descritos están relacionados con la configuración de servidores, con la protección de equipos mediante la actualización de antivirus y el proceso de préstamo de Laboratorios de Cómputo.

1. Marco Teórico

1.1 Seguridad Informática

Actualmente la seguridad es un factor importante en toda organización, y en mayor grado en aquellas cuya infraestructura de comunicaciones haga uso de Internet, por lo que se debe definir el desarrollo e implementación de niveles de seguridad que protejan cualquier sistema de información.

La Internet, intranets y extranets permiten una comunicación rápida y efectiva entre empleados, socios y usuarios potenciales para cualquier organización, sin embargo tanto la comunicación como la eficiencia en la misma pueden verse comprometidas, degradadas e incluso llegar a ser impedidas debido a un ataque informático, ya sea a las vías de comunicación o a la propia información que viaja en la red, de ahí la necesidad de asegurarlos.

Aunque la seguridad es un concepto muy amplio que se aplica a una gran cantidad de actividades, una primera aproximación al concepto de seguridad es la siguiente[1]: Seguridad es un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo mediante la implementación de reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera grupal o empresarial.

Esta definición involucran tres términos esenciales para el manejo de seguridad: peligro, daño, y riesgo. Se entiende como *peligro o daño* todo aquello que pueda afectar el funcionamiento directo o los resultados que se obtienen del sistema en cuestión; el *riesgo* es la posibilidad de que se genere un impacto determinado en un activo, en un dominio de, o en toda la organización.

Considerando lo anterior una posible definición de *seguridad de la información*[2] es: Conjunto de procesos, procedimientos, tareas y actividades implementados conjuntamente apoyados en elementos de cómputo y telecomunicaciones que permiten controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos (información, equipos, etc.) ubicados en un sitio específico, durante su estadía en un medio de almacenamiento o durante su transmisión, en sus aspectos de integridad, disponibilidad, confidencialidad y autenticidad.

De esta definición es importante resaltar lo siguiente:

- *Conjunto de procesos, procedimientos, tareas y actividades*, lo cual indica que la seguridad es un sistema complejo y requiere de la implementación de más de una técnica y herramienta de cómputo.

- *Implementados con elementos de cómputo y telecomunicaciones*; es muy importante el apoyo tecnológico aunque no es lo único. Muchas organizaciones o personas creen que con el simple hecho de comprar una herramienta tecnológica de apoyo a la seguridad es suficiente para tener seguridad. Por ejemplo, compran un firewall o un software antivirus y creen que con esto ya tienen seguras sus redes o equipo de cómputo, pero si no

configuran el firewall o el software antivirus para sus propias necesidades y no se tienen procedimientos permanentes de revisión para dichos elementos, políticas de seguridad, tareas periódicas de actualización, etc., ni el firewall ni el antivirus proporcionarán la seguridad necesaria para los recursos informáticos.

- *Que pongan en riesgo los recursos informáticos*. Actualmente, lo más importante para una organización es la información y por eso la seguridad informática ha tomado tanto auge, pero no es lo único a proteger ya que aquellos recursos físicos de cómputo como servidores, computadores, impresoras, dispositivos extraíbles, y por supuesto el recurso humano también deben ser protegidos.

1.2 Evolución histórica de la Seguridad Informática

Hablar de la evolución de la Seguridad Informática es hablar de la evolución del cómputo y las tecnologías de la información.

Cuando nace la informática las empresas contaban con un mainframe en un Centro de Cómputo, el cual era administrado por expertos que eran los únicos que tenían acceso a él. Allí la seguridad consistía en una seguridad física donde se garantizaba que los expertos fueran personal de confianza y que el lugar en donde estaba el mainframe tuviera las condiciones adecuadas referentes a instalaciones, medio ambiente y acceso físico[W1].

Continuando con la evolución, aparecen las terminales "tontas", las cuales son una simple extensión de la pantalla del servidor (inicialmente muy cerca del mainframe y luego ubicada hasta a varios kilómetros de distancia usando líneas de comunicación) permitiendo que más de una persona tuvieran acceso e hiciera uso del sistema. En este esquema, la seguridad, además de incluir el ambiente, las instalaciones y el acceso al mainframe, estaba relacionada con las personas que podían usar las terminales (las cuales generalmente eran un grupo selecto) y también se encontraba enfocada a garantizar que el mainframe tuviera la capacidad de permitir el trabajo multiusuario pero todavía sin tratar problemas complejos de autenticación de usuarios ni permisos para el uso de recursos.

En la siguiente etapa aparecen las computadoras personales con capacidad de almacenar datos en equipos cliente; en ese momento las cuestiones de seguridad se vuelven más complejas debido que los recursos informáticos no están en un sitio cerrado, fácil de custodiar y controlar, sino que están distribuidos por toda la organización y son usados por muchas más personas (aparece el concepto Cliente/Servidor).

Casi de forma paralela aparecen las Redes de Área Local (LAN) en donde las computadoras se interconectan entre sí y con los servidores, permitiendo la movilidad de información de un lugar a otro de una manera fácil y sencilla. En este escenario el tema de seguridad se vuelve muy relevante pues cualquier persona que tenga acceso a una computadora conectada a la red, puede obtener información de otros equipos o más aún podría enviar virus o software malicioso (ahora denomina malware) a través de la red comprometiendo así la disponibilidad de los servicios y datos que se encuentren almacenados tanto en las computadoras como en los servidores.

Al abrirse este acceso a las redes también se abren las brechas de seguridad, donde los primeros ataques fueron los virus informáticos.

Finalmente, con la aparición de las Redes de Área Mundial (WAN), y en particular con Internet donde ya no importa en dónde se esté o qué sistema operativo se tenga es posible acceder a otros equipos de cómputo y servidores (boom de las punto com). Esta nueva filosofía genera mayores retos en cuanto a seguridad de los recursos informáticos, ya que no sólo es posible recibir ataques (intentos de acceso ilegales, denegaciones de servicio, virus, etc.) desde dentro de las organizaciones sino también desde cualquier parte del mundo.

La historia de las computadoras y la virología informática no comienza con Windows ni con DOS, pues se remonta más atrás: el primer virus de computadora, un gusano que apareció en 1988, fue escrito para Unix. Sin embargo, la virología informática sólo comenzó a evolucionar con la aparición de millones de equipos funcionando con DOS y posteriormente con Windows; la evolución del malware refleja la evolución de la industria del cómputo en su conjunto: la popularidad de una plataforma puede medirse por el número de virus que la afectan.

La evolución del malware en el campo de la seguridad informática se ha incrementado en los últimos años[W2], por lo que hoy en día es uno de los principales problemas que se enfrentan en el ámbito computacional donde las variantes van desde aquel usuario esporádico de Internet hasta el más astuto dentro de la red.

Aunado al malware se generan otro tipo de ataques informáticos como el spam, ocasionado por software spyware, el cual espía las consultas a los sitios de Internet que generalmente frecuenta el usuario o por ejemplo, también el robo de información por medio de los keyloggers (spyware que recolecta todas y cada una de las teclas oprimidas por el usuario, incluidas claves de acceso).

Es indiscutible que el malware es cada vez más sofisticado y aprovecha las ventajas de la tecnología para ser más nocivo, rápido y cauteloso o sutil en la forma de engañar a sus víctimas; como consecuencia, la solución para contrarrestar estos ataques demora aún más.

Debido a la evolución y tendencia del malware surge la denominada criptovirología, que es la técnica de combinar los virus con el apoyo de la criptografía e investiga la forma de mejorar los programas maliciosos para hacer más daño, con la implementación de algoritmos criptográficos.

Un término que surge y tal parece que hoy en día se ocupa como técnica de los creadores de este tipo de software malicioso es el Ransomware el cual, originalmente, lo ocuparon los creadores de software donde no liberaban su código fuente o no permitían realizar todas las operaciones de su aplicación, hasta que se realizaba un pago para que el autor enviara la licencia o hiciera Open Source su herramienta. Sin embargo, y como ocurre en todo, hay gente que hace mal uso de las reglas para adecuarlas a su beneficio y dañar a terceros: ahora los desarrolladores de la criptovirología realizan software que daña y piden dinero para el envío de la solución.

Recordando la historia del primer gusano en Internet[W3], diseñado por Robert Morris, que se reproducía a sí mismo y aprovechando una falla en los sistemas de correo electrónico se auto-enviaba logró poner fuera de servicio más de 6,000 sistemas de correo electrónico en los Estados Unidos, es evidente que la investigación realizada sobre el hecho implicó un análisis detallado del protocolo de correo SMTP, aunado a largas horas de seguimiento de los mensajes entre los

diferentes destinos y, sobre todo, del conocimiento de la funcionalidad del gusano creado, lo cual implica una mayor especialización en conocimientos de cómputo, tanto para el ataque como para contrarrestarlo.

Con el avance de la tecnología, las fallas de seguridad o vulnerabilidades se fueron especializando: el *buffer overflow* (o desbordamiento de variables en tiempo de ejecución), los programas denominados *shellcodes* (códigos de programas que al inyectarse en la memoria de un dispositivo y ejecutarse, obtiene interfaz de comandos con altos privilegios), el *IP Spoofing* (la suplantación de dirección IP), la manipulación de la pila de protocolos, particularmente de TCP/IP y la inundación de redes o sistemas de comunicaciones con altas cantidades de paquetes (DoS), fueron la constante que pusieron en alerta a todas las organizaciones y los mecanismos de seguridad implementados para identificar y hacer frente a dichos ataques y tratar de mantener el control aparente del funcionamiento de sus infraestructura de cómputo y comunicaciones.

Finalizando los 90's e iniciando este nuevo milenio, siguieron apareciendo nuevas formas de ataques, por lo que comenzó el crack de las punto com. Los temas orientados a la web, la inyección de código SQL (Lenguaje de Consulta Estructurado), la suplantación de sitios web, el phishing (estafas por email), las fallas en las bases de datos, la manipulación de paquetes de comunicación (fragmentación patológica, paquetes malformados), la ingeniería inversa como estrategia para superar medidas de seguridad y control y nuevos gusanos, más elaborados y con capacidad de contagio y expansión más evidente, gracias a las conexiones vía Web y los códigos ejecutables embebidos en páginas, muestran un panorama más exigente y más elaborado para la implementación de herramientas de seguridad.

1.3 Normatividad de la Seguridad Informática

La Normatividad de la Seguridad Informática tiene como finalidad definir los criterios bajo los cuales se denotará que un sistema de información es seguro o no mediante una serie de estándares de seguridad a seguir.

Un Estándar de Seguridad establece los requerimientos de seguridad que debe cumplir un sistema de cómputo para calificarlo formalmente como un *sistema confiable certificado* y tiene como función especificar

- lo que se debe hacer
- los controles de seguridad que se requieren
- la definición de los controles de seguridad adecuados que se deben aplicar a cada elemento del entorno de la protección de la información

a fin de cubrir todos los activos de la organización y derivar en una Política de Seguridad confiable.

Para que un estándar sea implementado se debe apoyar en un proceso de gestión, el cual debe ser:

- Medible. Un estándar internacional puede ser evaluado por una tercera parte.
- Repetible. El sistema es repetible de una sede a otra, porque contiene una estructura de procesos única.
- Escalable. Los sistemas y procesos de gestión pueden ser diseñados centralizadamente y posteriormente ser distribuidos en cualquier sede de la organización.

1.3.1 Organismos internacionales enfocados a la Seguridad

Partiendo del principio que Internet es una red totalmente abierta y pública, sin ningún tipo de jerarquía establecida ni de autoridad central, donde el número de usuarios aumenta día a día de manera espectacular al igual que el tipo de operaciones que sobre ella se realizan, es fácil imaginar la inseguridad de los datos transmitidos y almacenados en los equipos conectados a ella.

Considerando la problemática anterior, durante las últimas décadas se han instaurado organismos internacionales encargados de la denominada "gobernanza en Internet"[W4], los cuales se encuentran avocados a la generación y vigilancia en la aplicación de estándares para la instalación, administración, desarrollo y operación de sistemas informáticos, favoreciendo con esto la implementación de seguridad en el manejo de los mismos; sin embargo, un estándar no nos garantiza seguridad absoluta en los sistemas informáticos, dado que cada uno tiene su particularidad y su propio nivel de complejidad.

Los aspectos a los cuales se encuentran enfocados estos organismos internacionales se muestran en la Figura 1-1.

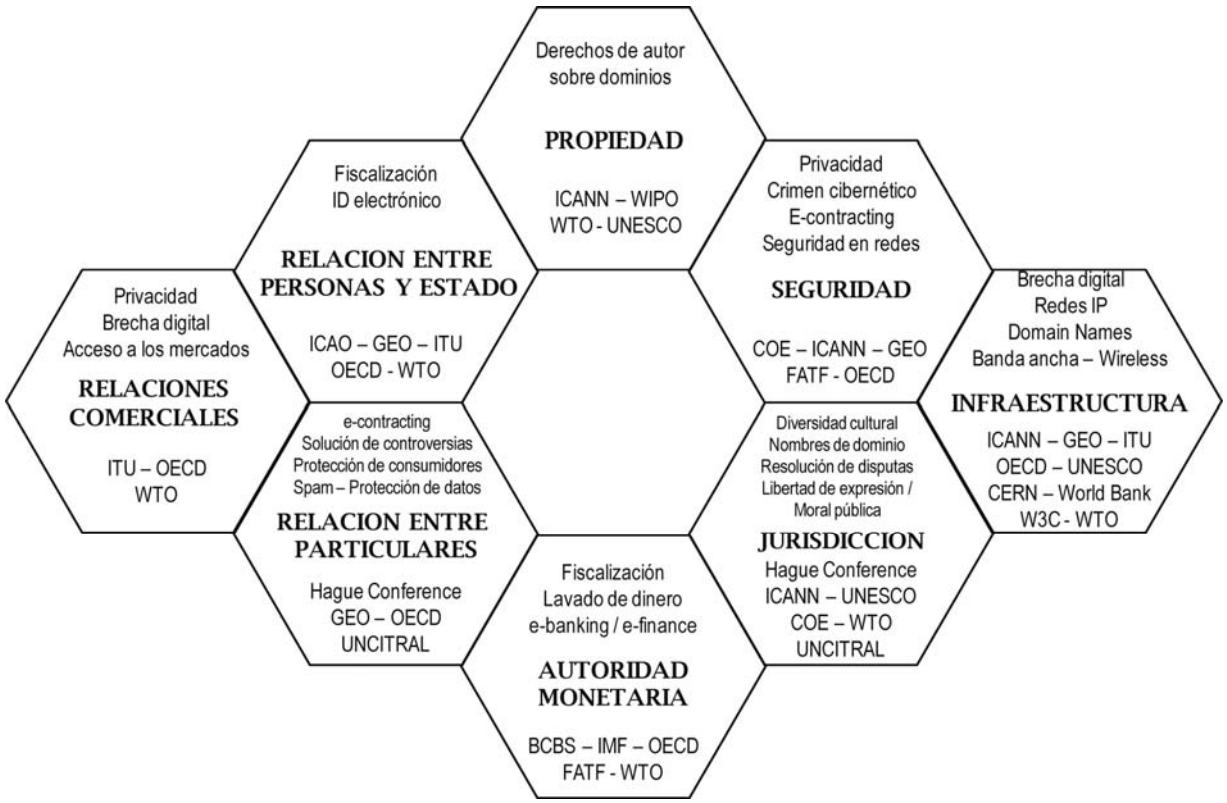

Figura 1-1. Gobernanza en Internet

De estos, los organismos que mayor influencia tienen sobre la Gobernanza en Internet son:

- IETF (Fuerza de Tarea de Ingeniería en Internet)
  Contribuye a la ingeniería y la evolución de las tecnologías de Internet mediante estándares, normas e iniciativas sobre la operación, funcionamiento y seguridad de la red.

- ICANN (Corporación de Internet para la Asignación de Nombres y Números)
  Realiza la coordinación técnica de Internet en la asignación de nombres de dominio y parámetros de protocolos.

- ITU (Unión Internacional de Telecomunicaciones)
  Tiene como objetivo la aprobación y establecimiento de estándares para redes y servicios de telecomunicaciones, promoviendo y expandiendo el uso de las redes de cómputo en IP.

- Comisión de las Naciones Unidas en Derecho Comercial Internacional
  Se encarga de la unificación de leyes de comercio internacional aplicables al comercio electrónico y sistemas de negociación y pagos internacionales.

- W3C (Consorcio del World Wide Web)
  Encabeza la evolución tecnológica del WWW.

Ligado a estas instituciones, existen las correspondientes a la definición y estandarización de las TIC's, dentro de las cuales se encuentran las siguientes:

- IETF (Fuerza de Tarea de Ingeniería en Internet)
  Realiza la definición de estándares y normas para la operación de protocolos y sistemas en Internet. Utiliza las siguientes tecnologías: Internet, Internet 2, IPv4, IPv6, Audio, video y colaboración en red.

- IAB (Consejo de Arquitectura de Internet)
  Realiza la supervisión de las actividades de la IETF y coordina las RFC´s mediante estándares de red, estándares de protocolos de comunicación y estándares de arquitectura de red.

- Fuerza de Tarea de Investigación en Internet
  Promueve la importancia de la evolución en Internet a través de grupos de trabajo especializados. Utiliza las tecnologías de anti-spam, encriptamiento, tolerancia a fallos, conexiones punto a punto, métricas de red así como optimizaciones de movilidad.

- Internet Society
  Su objetivo primordial es el asegurar el desarrollo y evolución abiertos de Internet y que la red beneficie a toda la gente a través de la interconectividad, seguridad y capacitación.

- IEEE (Instituto de Ingenieros en Electricidad y Electrónica)
  Es la autoridad en desarrollo de estándares y normas para Internet.

- ETSI (Instituto Europeo de Estándares en Telecomunicaciones)
  Realiza la producción de estándares de telecomunicaciones.

- IANA (Autoridad de Internet para Asignación de Números)
  Lleva a cabo la asignación de rango de direcciones y nombres a través de los registros regionales, nacionales y locales.

- Alianza Mundial de Tecnología y Servicios de la Información
  Su principal objetivo es compartir el conocimiento de TICs y promover su adecuada aplicación mediante el incremento de competencias, protección a la propiedad intelectual, promover la capacitación, incrementar la seguridad de la información, y propiciar el comercio electrónico y el crecimiento de Internet.

- AMITI (Asociación Mexicana de la Industria de Tecnologías de la Información)
  Realiza la integración de las TI en México a través de la difusión y aprovechamiento de las TI a todos los niveles de la sociedad capacitando en su uso, promoviendo su desarrollo y realizando la vinculación con la Academia.

Como podemos ver, existe más de un organismo que promueve la estandarización, comunicación y buen uso de Internet y las Tecnologías de Información, sin embargo, los problemas de seguridad no son necesariamente técnicos, por lo que también se debe proteger a los sistemas de información de otro tipo de amenazas, que van desde desastres naturales hasta la ingeniería social.

1.3.2 Estándares de Seguridad a través de la historia

La estructura de los estándares define lo que se debe hacer para proteger la información y respaldar los requerimientos de la política de seguridad de la información. En [3], [4] y [5] se presenta en detalle una explicación de los diferentes estándares que se han desarrollado a lo largo de la historia.

A mediados de los años 80 el Departamento de Defensa de los Estados Unidos desarrolló el Trusted Computer System Evaluation Criteria (TCSEC) [6], el cual proporciona especificaciones de seguridad relativas al sistema operativo y sistemas manejadores de bases de datos. En la siguiente década, otros países tomaron iniciativas análogas y dirigidas a desarrollar nuevos criterios de evaluación, construidos sobre los conceptos del TCSEC americano pero siendo más flexibles y adaptables a la evolución de las TI. En 1991, en Europa se publica el Information Technology Security Evaluation Criteria (ITSEC) [7] por parte de la Comisión Europea después del esfuerzo conjunto de Francia, Alemania, Holanda, y Reino Unido para la descripción de un proceso formal y bien definido de evaluación de la seguridad en las TI. Por otra parte, en Canadá, se publica la Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [8] como una continuación de las aproximaciones de ITSEC y TCSEC (1993).

En Estados Unidos y también en 1993, se publica el borrador de los Federal Criteria for Information Technology Security (FC-ITS) [9] como una segunda aproximación que combina los conceptos americanos y europeos en lo que a criterios de evaluación se refiere.

El Instituto de Estándares Británico publicó la norma BS-7799 en 1995. Este documento fue presentado a aprobación por la International Organization for Standardization (ISO) para producir un estándar internacional de seguridad de la información.

Paralelamente y desde 1990, en la ISO se habían iniciado algunos trabajos para desarrollar un conjunto de estándares internacionales, con ámbito general, para los criterios de evaluación (ISO/IEC 15408) de la seguridad de los sistemas de información.

La ISO también desarrolló la norma ISO-15408 en 1999, que define estándares de medidas de seguridad TI que se implementan en el hardware, firmware o software. La norma ISO-15408 ignora toda medida de seguridad que esté fuera del dispositivo para el cual se ha aplicado, aunque reconoce que se puede aplicar seguridad significativa a través del uso de medidas administrativas, como los controles a las organizaciones, al personal, controles de tipo físico y de procedimiento.

En el año 2000, la ISO publicó una versión internacional de la BS-7799, conocida como ISO-17799, que eliminó algunos elementos específicos de la ley británica.

Las normas hoy conocidas como "Common Criteria" son el resultado de una serie de esfuerzos enfocados al desarrollo de criterios para la evaluación de la seguridad en las tecnologías de la información; son una certificación de evaluación de seguridad a nivel internacional apoyada por el Communications-Electronics Security Group (CESG) con el objetivo de reemplazar con un solo estándar los criterios previos.

El objetivo final es que la certificación obtenida a través de un organismo certificador tenga que ser reconocida por otros certificadores reduciendo así el costo para desarrolladores y aumentando la confianza del usuario. Este trabajo comenzó en 1993 y se produjo la versión 1.0 de Criterios Comunes en enero 1996. Esta versión fue trabajada y refinada apoyada por un periodo de revisión y pruebas de usuario; el borrador final de la versión 2.0 fue publicado en diciembre de 1997. La versión 2.0 de los Criterios Comunes fue finalizada en mayo 1998 y entregada a la ISO para su aceptación como un estándar internacional. La Versión 2.1 de los Criterios Comunes es equivalente al Estándar Internacional de ISO 15408.

En mayo de 2002, tras dos años de negociaciones entre administraciones e industria, los gobiernos de EEUU, Canadá, Francia, Alemania y Reino Unido firman un acuerdo histórico por el que se comprometen a reconocer los resultados de todas aquellas evaluaciones que se hiciesen siguiendo las directrices de los Criterios Comunes en la forma de los denominados "Protection Profiles". Los objetivos de estas medidas son:

- Asegurar que la evaluación de productos de las Tecnologías de la Información (TI) se realiza según estándares de calidad y son vistos como argumentos para fundamentar la confianza en la seguridad de dichos productos.
- Aumentar la disponibilidad de productos TI de calidad y de seguridad probada, así como la existencia de "Protection Profiles" de uso nacional.
- Eliminar las dobles evaluaciones; es decir, que los productos TI y los "Protection Profiles" que tienen un "Common Criteria Certificate" pueden obtenerse de una sola vez.
- Mejorar continuamente la eficiencia, efectividad y los costes de las evaluaciones de seguridad y de los procesos de validación/certificación.

El acuerdo especifica las condiciones en las que los participantes aceptarán los resultados de las evaluaciones de la seguridad en productos TI y define un comité de gestión compuesto por representantes de cada país firmante, cuya misión es desarrollar el acuerdo y dar guía a los

subordinados esquemas nacionales relacionados con la evaluación y validación de los productos TI.

Sin embargo, la complejidad de los sistemas de información y productos a evaluar es ya tan significativa, que un criterio de evaluación ideal y una metodología humanamente perfecta no podrían atender a todos los riesgos o eventualidades posibles, por lo que para cada caso se deben implementar criterios específico y acordes a las necesidades propias de la organización.

A continuación se describen cada una de las recomendaciones de seguridad en sistemas de Información:

1.3.2.1 TCSEC / Libro Naranja

Los TCSEC (Trusted Computer System Evaluation Criteria) comúnmente son conocidos como el Libro Naranja [W5].

Fueron desarrollados por el NCSC (National Computer Security Center) de la NSA (National Security Agency) del Departamento de Defensa de EEUU y adoptados como estándar en el año de 1985. Suministra especificaciones de seguridad relativas a sistemas operativos; actualmente se está trabajando en su modernización para ampliar su alcance hacia las aplicaciones, bases de datos y comunicaciones (redes y bases de datos confiables).

Los TCSEC tienen por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense; esta política se centra, fundamentalmente, en el mantenimiento de la confidencialidad de la información clasificada a nivel nacional. Ayuda a identificar requerimientos específicos de seguridad para la planificación y la construcción de sistemas operativos mediante las siguientes acciones:

- Suministrar normas de seguridad a los fabricantes.
- Definir métricas de evaluación y certificación.
- Establecer condiciones para la adquisición de sistemas operativos.

Dentro de las partes implicadas en esta construcción se encuentran:

- Patrocinador.
- Productor.
- Instalaciones de Evaluación.
- Comisión Nacional de Certificación.
    - Acreditación de Instalaciones.
    - Supervisión de la Evaluación.
    - Revisión de Informes Técnicos.
    - Publicación de Certificados.

Los TCSEC se integran por un conjunto de cuatro Divisiones (D, C, B, A) divididas a su vez en siete clases, generando así un número similar de clases de criterios de evaluación: D, C1, C2, B1, B2, B3 y A1.

Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van creciendo en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 el más elevado.

Todas las clases incluyen tanto requisitos de funcionalidad (conjunto de funciones de seguridad) como de confianza (efectividad y corrección), tal como se muestra en la Tabla 1-1.

<table>
<tr><th>D</th><th>C</th><th>B</th><th>A</th></tr>
<tr><th>Protección Mínima</th><th>Protección Discrecional del Hardware</th><th>Protección Obligatoria</th><th>Protección Verificada</th></tr>
<tr><td rowspan="2">Sin Seguridad.
El sistema por sí mismo es no confiable.
No se dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe autentificación por parte de los usuarios y sus directivos respecto a los accesos a la información almacenada en el equipo de cómputo</td><td>C1. Limitaciones de accesos a directorios y archivos mediante la identificación y autenticación.
Se determinan los derechos de acceso a programas e información que tiene cada usuario al implementar el acceso discrecional.</td><td>B1. Equivalente al C2 pero con una mayor protección para cada archivo
• Etiquetas
• Control de acceso obligatorio (pruebas de penetración)</td><td rowspan="2">A1. Protección verificada. En la práctica, es lo mismo que el nivel B3, pero la seguridad debe estar definida en la fase de análisis del sistema
• Diseño, especificación y verificación (verificación formal).
• Distribución confiable.
• Análisis de Cobertura de canales (Análisis formal de cobertura de Canales).</td></tr>
<tr><td>C2. Acceso controlado a los Sistemas de Información con base no sólo en los permisos, sino también en los niveles de autorización.
Se realiza la implementación de auditorías al sistema y su arquitectura, así como pruebas de seguridad.</td><td>B2. Los sistemas deben estar diseñados para ser resistentes al acceso de personas no autorizadas.
• Diseño, especificación y verificación
• Análisis de cobertura de canales
• Manejo confiable
• Recuperación confiable</td></tr>
</table>

		B3. Dominios de seguridad. Los sistemas deben estar diseñados para ser altamente resistentes a la entrada de personas no autorizadas • Configuración de operación • Pruebas de seguridad • Arquitectura del sistema (Ingeniería de software)	

Tabla 1-1. Divisiones TCSEC

Actualmente, la responsabilidad sobre la seguridad de sistemas de información la ostenta un organismo civil: el National Institute of Standards and Technology (NIST).

➢ National Institute of Standards and Technology (NIST)

El Instituto Nacional de Estándar y Tecnología, es una Agencia Federal (no regulatoria) del Departamento de Comercio de los Estados Unidos. Fue fundada en 1901 y tiene como misión promover la innovación y la competitividad industrial. Para lograr esto, cuenta con varios programas cooperativos, entre los cuales destacan:

- *Los Laboratorios NIST,* los cuales conducen investigaciones cuyo objetivo es avanzar sobre la infraestructura tecnológica, abordándola desde distintos ámbitos a fin de lograr mejorar el uso, confiabilidad y seguridad de los sistemas de información, computadoras y redes de computadoras.
- *El Programa de Extensión Manufacturera*: Este programa establece asociaciones con pequeñas empresas manufactureras, a fin de apoyarlas y orientarlas tecnológicamente. Algunos de los aspectos que apoya este programa son las herramientas para el aprendizaje del comercio electrónico y la seguridad de la infraestructura tecnológica.
- *El Programa de Avance Tecnológico*. Una propuesta que permite al NIST brindar asesoría avanzada, especialmente concebida para el sector tecnológico.

El NIST provee además estándares y herramientas para todos estos programas, permitiendo la evaluación de riesgos relacionados con las Tecnologías de Información. En los últimos años este Instituto ha favorecido activamente el desarrollo de modelos comúnmente utilizados hoy en día, como por ejemplo los orientados hacia la comunicación de transacciones electrónicas (comercio electrónico vía Internet, cajeros automáticos, etc.), entre otros.

1.3.2.2 Information Technology Security Evaluation Criteria (ITSEC)

El ITSEC (Information Technology Security Evaluation Criteria) surgió de la conjunción de varios sistemas europeos de criterios de seguridad en TI, y es considerado como el equivalente europeo del Libro Naranja, pero más moderno y con mayor alcance; comúnmente se le conoce como Libro Blanco. Evalúa la seguridad de sistemas, productos TI o partes de estos.

Los criterios establecidos en el ITSEC permiten seleccionar funciones de seguridad arbitrarias (objetivos de seguridad que el sistema bajo estudio debe cumplir teniendo presentes las leyes y reglamentaciones vigentes).

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada, E1 el punto de entrada por debajo del cual no existe una confianza útil, y E6 el nivel de confianza más elevado. Por ello, los presentes criterios pueden aplicarse a una gama de posibles sistemas y productos más amplia que los del TCSEC.

En general, a funcionalidad idéntica y a nivel de confianza equivalente, un sistema goza de más libertad arquitectónica para satisfacer los criterios de ITSEC que los de TCSEC. La correspondencia que se pretende entre los criterios ITSEC y las claves TCSEC se muestra en la Tabla 1-2.

Criterios ITSEC		**Claves TCSEC**
Funcionalidad	**Confianza**	
	E0	D
F-C1	E1	C1
F-C2	E2	C2
F-B1	E3	B1
F-B2	E4	B2
F-B3	E5	B3
F-B3	E6	A1

Tabla 1-2. Correspondencia de criterios ITSEC y claves TCSEC

a) Clases de Funcionalidad

Las funciones dedicadas a la seguridad que un objeto de evaluación (TOE, Target Of Evaluation) debe ofrecer pueden presentarse explícitamente, mediante referencia a una o más clases de funcionalidad predefinidas, o mediante referencia a una norma aceptada que defina una funcionalidad de seguridad

En la Tabla 1-3 se presentan las clases de funcionalidad para el ITSEC:

Clase	Funcionalidad
F-C1	Proporciona un control de acceso discrecional.
F-C2	Proporciona un control de acceso discrecional más específico que la clase C1, imputando directamente las acciones a los usuarios mediante procedimientos de identificación, auditoria de sucesos relevantes para la seguridad y aislamiento de recursos.
F-B1	Además del control de acceso discrecional, introduce funciones para mantener etiquetas de sensibilidad y se sirve de ellas para imponer un conjunto de normas obligatorias de control de acceso a todos los sujetos y objetos de almacenamiento que están bajo su control. Es posible el etiquetado con precisión de información exportada.
F-B2	Amplía el control obligatorio de acceso a todos los sujetos y objetos y refuerza los requisitos de autenticación de la clase B1.
F-B3	Además de las funciones de la clase B2, proporciona funciones de soporte a roles diferenciados de administración de seguridad y la auditoria se amplía para señalar los sucesos relevantes para la seguridad.
F-IN	Dirigida a TOE con requisitos de alta integración para datos y programas. Estos requisitos podrán ser necesarios en las bases de datos TOE.
F-AV	Establece requisitos elevados para la disponibilidad de un TOE por completo o de funciones especiales. Dichos requisitos son importantes para TOE que controlen procesos de fabricación.
F-DI	Establece requisitos elevados relativos a la protección de la integridad de los datos durante el intercambio de los mismos.
F-DC	Dirigida a los TOE con elevadas demandas relativas a la confidencialidad de los datos durante el intercambio de los mismos. Un ejemplo para esta clase es el dispositivo criptográfico.
F-DX	Dirigida a redes con elevadas demandas de confidencialidad e integridad de la información intercambiada. Este es el caso, por ejemplo, cuando debe intercambiarse información sensible a través de redes inseguras.

Tabla 1-3. Clases de funcionalidad de ITSEC

El objetivo del proceso de evaluación es permitir al evaluador la preparación de un informe imparcial en el que se indique si el sistema bajo estudio satisface o no su meta de seguridad en base al nivel de confianza determinado por el nivel de evaluación indicado.

b) Niveles de Evaluación

Los niveles de evaluación se definen dentro del contexto de los criterios de corrección. La *evaluación* de la corrección investiga si las funciones y mecanismos dedicados a la seguridad están implementados correctamente. La *corrección* se aborda desde el punto de vista de la construcción del objeto de evaluación (TOE, producto o sistema que va a evaluarse). Se han definido siete niveles de evaluación, denominados E0 a E6, que representan grados crecientes de confianza en la corrección; estos se presentan en la Tabla 1-4.

Nivel de Evaluación	Grado de Confianza
E0	Representa un aseguramiento inadecuado. No se emite certificado
E1	A este nivel deberán existir una meta de seguridad y una descripción informal del diseño arquitectónico del TOE. Las pruebas funcionales deberán mostrar que el TOE satisface su meta de seguridad
E2	Además de los requisitos correspondientes al nivel E1, deberá existir una descripción informal del diseño detallado. Deberán evaluarse las pruebas de la realización de pruebas funcionales. Deberá existir un sistema de control de la configuración y un procedimiento de distribución aprobado
E3	Además de los requisitos correspondientes al nivel E2, deberá evaluarse el código fuente y/o los esquemas del hardware correspondientes a los mecanismos de seguridad. Deberán evaluarse las pruebas de la realización de pruebas de estos mecanismos
E4	Además de los requisitos correspondientes al nivel E3, deberá existir un modelo formal subyacente de política de seguridad que soporte la meta de seguridad. Deberán especificarse en estilo semi-formal las funciones dedicadas a la seguridad, el diseño arquitectónico y el diseño detallado
E5	Además de los requisitos correspondientes al nivel E4, deberá existir una estrecha correspondencia entre el diseño detallado y el código fuente y/o los esquemas de hardware
E6	Además de los requisitos correspondientes al nivel E5, deberán especificarse en estilo formal las funciones dedicadas a la seguridad y el diseño arquitectónico, de forma coherente con el modelo formal subyacente de política de seguridad especificado

Tabla 1-4. Niveles de Evaluación de ITSEC

1.3.2.3 Information Technology Security Evaluation Manual (ITSEM)

El Information Technology Security Evaluation Manual (ITSEM) es el Manual de evaluación de la seguridad de TI que forma parte del ITSEC versión 1.2 y cuya misión es describir cómo aplicar los criterios de evaluación del ITSEC.

El objetivo específico del ITSEM es asegurar que existe un conjunto completo de métodos de evaluación de sistemas de seguridad que complemente al ITSEC. Contiene métodos y procedimientos de evaluación suficientemente detallados para ser aplicados a evaluaciones de seguridad realizadas tanto en el sector privado como en el público.

a) Métodos definidos por el subcomité 27 del JTC-1 de la ISO/IEC

La ISO, junto con la International Electrotechnical Commission (IEC), ha creado un Joint Technical Comittee (JTC-1) para abordar un amplio rango de estándares aplicables a las tecnologías de la información, incluida la seguridad. Se han establecido varios subcomités para el desarrollo de estándares, de los cuales el SubComité 27 (SC27) es el más relevante en cuanto a técnicas de seguridad se refiere. La lista de todos estos subcomités se detalla a continuación:

- SC6 Núcleo de seguridad. Capas OSI 3 y 4.
- SC14 Representación de elementos de datos. EDI.
- SC17 Tarjetas inteligentes y de identificación.
- SC18 Sistemas ofimáticos. Manejo de mensajes, oficina distribuida, arquitectura de seguridad de documentos compartidos.
- SC21 Seguridad de las capas altas del modelo OSI. Bases de datos, gestión de directorios y archivos, seguridad de FTAM y TP.
- SC22 Lenguajes.
- SC27 Técnicas de seguridad. Criptografía, etc. Incluye autentificación, integridad, no repudio, modos de operación, control de acceso y registro de algoritmos.

b) Métodos definidos por la European Computer Manufacturing Association (ECMA)

- TC22 Bases de datos.
- TC29 Seguridad de la arquitectura de documentos compartidos.
- TC32 Protocolos y capas bajas del modelo OSI.

c) Norma ISO 7498-2 (OSI, Security Architecture)

Esta norma define el concepto de Arquitectura de Seguridad, compuesta por servicios que deben ser implementados cuando se trabaja en un entorno de sistemas abiertos. Describe la selección, colocación y utilización de los servicios de seguridad y mecanismos en las capas superiores (aplicación, presentación y reunión de capas) del modelo de referencia OSI.

Los cinco servicios enumerados en la norma ISO 7498-2 son los siguientes:

- autenticación (incluyendo entidad y el origen de autenticación).
- control de acceso.
- confidencialidad de los datos.
- integridad de los datos.
- no repudio.

1.3.2.4 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

El CTCPEC es un estándar de seguridad publicado en 1993 por el Communications Security Establishment a fin de proporcionar un criterio de evaluación para las TI. Es una combinación del TCSEC y de los resultados del ITSEC.

Este estándar verifica la correcta implementación del producto basándose en las políticas de seguridad establecidas para ello, por lo que se aplica completamente a todos los servicios del producto bajo evaluación.

Requerimientos de evaluación:

- Arquitectura
- Desarrollo ambiental
- Desarrollo de evidencias
- Ambiente operacional
- Documentación
- Seguridad
- Seguridad en las pruebas

Los servicios de funcionalidad requeridos se indican el la Tabla 1-5.

Servicio de Funcionalidad	Requerimiento
Confidencialidad	Cobertura de canales Discrecional Obligatoria Reuso de objetos
Integridad	Dominio de Integridad Discrecional Obligatoria Física Rollback (protección de respaldos) Separación de funciones Autopruebas
Disponibilidad	Contención Tolerancia a fallas Robustez Recuperación
Auditoria	Registros Identificación y autentificación Rutas confiables

Tabla 1-5. Servicios de funcionalidad CTCPEC

1.3.2.5 Federal Criteria for Information Technology Security (FC-ITS)

Es una versión preliminar que combina los conceptos europeos y americanos en cuanto a criterios de evaluación para sistemas seguros y confiables a fin de reemplazar el TCSEC.

1.3.2.6 ISO 15408

El estándar ISO 15408 define criterios comunes para la evaluación de la seguridad de tecnologías de la información. Estos criterios evalúan el funcionamiento usando niveles divididos en dos grandes grupos: funcionalidad y seguridad [10].

a) Clases de Requisitos funcionales

- Security audit. (FAU) en el sentido de auditabilidad de la seguridad.
- Communication (FCO) que contempla requisitos para el aseguramiento de la identidad de las partes participantes en el intercambio de datos y el no rechazo (No repudio).
- Cryptographic support (FCS). Esta clase se utiliza cuando el TOE implanta funciones criptográficas en el hardware, firmware o software.
- User Data Protection (FDP) dirigida a la protección de datos de los usuarios.
- Identification and Authentication (FIA) trata la verificación de la identidad del usuario.
- Security Management (FMT) Contempla los requisitos de tiempo para la propagación de atributos de seguridad (por ejemplo revocación, autorización por tiempo limitado) en un entorno distribuido.
- Privacy (FPR) clase basada en el conocimiento actual de las técnicas sobre privacidad.
- Protection of the Trusted Security Functions (FPT) se centra en la integridad y gestión de los mecanismos que proporcionan las funciones de seguridad del TOE.
- Resource Utilisation (FRU) enfocado a la disponibilidad de los recursos (procesador, memoria, etc.).
- TOE Access (FTA) referente a los requisitos de identificación y autenticación para controlar el establecimiento de una sesión de usuario.
- Trusted Path/Channels (FTP) proporciona requisitos referentes a los distintos canales de comunicación seguros.

b) Clases de Requisitos de seguridad

- Configuration Management (ACM) incluye los requisitos dirigidos a asegurar la integridad de los parámetros de configuración de forma que únicamente los usuarios autorizados puedan cambiarlos.
- Delivery and operation (ADO) proporciona los requisitos para la correcta distribución, instalación y puesta en operación del TOE.
- Development (ADV) contiene requisitos para representar las funciones de seguridad del TOE (TSF) a diversos niveles de abstracción desde la interfaz funcional hasta la implementación.
- Guidance documents (AGD) proporciona los requisitos para los documentos: guía del usuario y guía del administrador para administrar/utilizar el TOE de la forma que proporcione la seguridad para la que fue diseñado.
- Life cicle support (ALC) en el aspecto de establecer la disciplina y control en el proceso de refinamiento del TOE durante su desarrollo y mantenimiento.

- Tests (ATE) mediante el test se determina si las funciones de seguridad del TOE (TSF) muestran las propiedades necesarias para satisfacer los requisitos funcionales del PP/ST.
- Vulnerability assessment (AVA) comprende, entre otros, el análisis de la existencia de canales ocultos que permitan ser explotados para violar la seguridad, la incorrecta o mala utilización de la configuración del TOE, test de penetración que exploten las vulnerabilidades.

De manera general, los niveles para la evaluación de seguridad se indican en la Tabla 1-6.

Nivel	Objetivo
EAL 1	TOE Funcionalidad probada Es aplicable cuando se requiere tener cierta confianza de la operación correcta y, donde además, las amenazas a la seguridad no son vistas como serias. Proporciona un análisis del comportamiento de las funciones de seguridad, utilizando especificaciones de funcionalidad e interfaz del TOE. El análisis es apoyado por pruebas independientes de las funciones de seguridad
EAL 2	TOE Estructuralmente Probado Este nivel es aplicable en circunstancias donde los desarrolladores o los usuarios requieren un nivel de bajo a moderado con respecto a la seguridad de garantía independiente, en ausencia de disponibilidad para preparar el registro de desarrollo completo. La evaluación debe ser independiente de las funciones de seguridad, del desarrollo de pruebas de la caja negra, y del desarrollo para encontrar vulnerabilidades obvias.
EAL 3	TOE Probado y verificado metódicamente Permite a un desarrollador aplicado y minucioso, alcanzar una máxima garantía de ingeniería de seguridad positiva en el diseño de la aplicación. El análisis del TOE es apoyado por pruebas de "caja gris" y una confirmación independiente de los resultados de las pruebas realizadas, así como evidencia de búsquedas de vulnerabilidades obvias. También se requiere del desarrollo de controles del entorno y administración de configuración del TOE.
EAL 4	Diseñado, probado y revisado metódicamente Este nivel le permite a un desarrollador alcanzar máxima seguridad de ingeniería de seguridad positiva basadas en buenas prácticas de desarrollo comercial. El análisis es apoyado por el diseño de bajo nivel de los módulos del TOE, así como por un subconjunto de la implementación. Los controles desarrollados se apoyan en el modelo de ciclo de vida de sistemas, herramientas de identificación, y la administración de configuración automatizada. Las pruebas son apoyadas por una búsqueda independiente de vulnerabilidades obvias.

EAL 5	Diseñado y probado semi-formalmente El análisis incluye todo el proceso de implementación. La garantía de seguridad es apoyada por un modelo formal y una presentación semi-formal de la especificación funcional del TOE, así como por un alto nivel de diseño. La búsqueda de vulnerabilidades debe garantizar una relativa resistencia a ataques de penetración. También se requiere un análisis de canal y del diseño modular.
EAL 6	Diseño verificado y probado semi-formalmente El análisis del diseño se apoya en una aproximación modular y evolutiva, así como por una presentación estructurada de la implementación del TOE. La búsqueda independiente de vulnerabilidades debe asegurar una alta resistencia a ataques de penetración. La búsqueda de conversión de canales debe ser sistemática. El entorno de desarrollo y los controles de administración de la configuración deben estar más fortalecidos.
EAL 7	Diseño verificado y probado formalmente Este nivel proporciona garantía mediante un análisis de las funciones de seguridad, usando una especificación funcional y de interfase completa, documentación guía, los diseños de alto y bajo nivel del TOE, y una presentación estructurada de la implantación, para entender el comportamiento de la seguridad. Se requiere la evidencia de desarrollo de pruebas de caja blanca así como requerimientos de confirmación completa independiente de los resultados de las pruebas realizadas por el desarrollador. La complejidad del diseño debe ser minimizada

Tabla 1-6. Niveles de Evaluación de Seguridad ISO 15408

1.3.3 Normas de Seguridad de la Información

1.3.3.1 Norma UNE-ISO/IEC 17799

Esta norma tiene su origen en la norma británica BS7799-1, la cual constituye un código de buenas prácticas para la Gestión de la Seguridad de la Información de cualquier organización cuyas actividades dependan de su información o de su infraestructura de información, la cual puede ser aplicada independientemente de su tamaño o sector[5].

Esta norma viene asociada con otras dos: la ISO 13335 - Guía para Administración de la Seguridad de Información y la ISO 15408 - Criterios para la Seguridad Informática.

La norma técnica fue redactada intencionalmente para ser imparcial respecto a una solución de seguridad específica, ya que las recomendaciones técnicas de esta norma son neutrales en cuanto a la tecnología; por ejemplo, la norma discute la necesidad de contar con firewall, pero no profundiza sobre los tipos de firewall.

Considerando que el propósito de la norma es garantizar la confidencialidad, la integridad y la disponibilidad de la información distribuida a través de la infraestructura de telecomunicaciones, define diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información, 36 objetivos de control y 127 controles[11], sin embargo tiene la gran desventaja de no ser certificable.

Los Dominios de Control de esta Norma se listan a continuación:

1. Política de Seguridad de la Información
   - Seguridad organizacional
   - Infraestructura
   - Acceso externo
   - Outsourcing

2. Aspectos organizacionales de la seguridad

3. Clasificación y control de activos
   - Clasificación de la información
   - Responsabilidad de acceso

4. Seguridad asociada al personal
   - Funciones y responsabilidades de la seguridad de la información
   - Capacitación al usuario
   - Respuesta a incidentes

5. Seguridad física y del entorno
   - Áreas protegidas
   - Seguridad del equipo
   - Controles generales

6. Gestión de comunicaciones y operaciones
   - Procedimientos operativos y responsabilidades operativas
   - Planeación y aprobación de sistemas
   - Protección contra software malicioso
   - Tareas de reorganización - organización y administración de sistemas
   - Administración de redes
   - Administración y seguridad de las medios de almacenamiento
   - Intercambio de información y software

7. Control de Accesos
   - Requerimientos de la empresa
   - Administración de accesos de usuario
   - Responsabilidades del usuario
   - Control de acceso a la red
   - Control de acceso al sistema operativo
   - Control de acceso a las aplicaciones
   - Monitoreo de acceso y uso de sistemas
   - Computación móvil y trabajo a distancia

8. Desarrollo y mantenimiento de sistemas
   - Requerimientos de seguridad de los sistemas
   - Seguridad de las aplicaciones
   - Controles criptográficos
   - Seguridad de los archivos del sistema
   - Seguridad en los procesos de desarrollo y soporte

9. Gestión de la continuidad del negocio
   - Sistemas, redes, aplicaciones, personal, instalaciones y comunicaciones

10. Cumplimiento de la normatividad legal o conformidad
    - Cumplimiento de los requisitos legales
    - Cumplimiento de la seguridad e informes de cumplimiento técnico
    - Aspectos de la auditoria de sistemas

El estándar ISO 17799 indica los objetivos de seguridad a alcanzar, pero tiene como desventaja que no detalla el proceso de implementación.

La Figura 1-2 muestra los dominios de control y su ámbito de acción dentro de cualquier organización, así como los tipos de seguridad a implementar.

Figura 1-2. Dominios de Control de la Norma ISO/IEC 17799

Para su implementación, se requiere que todas las unidades operativas de la organización se involucren, siendo el área de cómputo la mayormente involucrada.

Cuando se implementa este estándar, el esfuerzo es muy grande al inicio de su implementación, pero conforme pasa el tiempo la documentación sólo debe cambiarse si se introduce un nuevo sistema, red, aplicación, ley o reglamentación, o existe un cambio en los mismos.

1.3.3.2 Norma UNE 71502

- Se basa en los controles y objetivos de control de la norma UNE-ISO/IEC 17799.
- Contiene las especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) referentes al Establecimiento, Implantación, Documentación y Evaluación, es decir, el componente documental del sistema.

1.3.3.3 OCTAVE

OCTAVE (Operational Critical Threat, Asset and Vulnerability Evaluation) es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo; permite evaluar las vulnerabilidades y amenazas que existen sobre los activos y operaciones críticas de una organización[W6]. Los creadores de OCTAVE provienen del Carnegie Mellon, renombrada universidad americana enfocada a la seguridad de sistemas de información, y fundaron el Computer Emergency Response Team (CERT) que se especializa en sistemas de intrusión.

Una evaluación efectiva de riesgos en la seguridad de la información considera aspectos tanto organizacionales como técnicos y legales, ya que examina cómo se emplea la infraestructura de uso cotidiano por parte de la gente relacionada con la organización (Figura 1-3). La evaluación es de vital importancia para cualquier iniciativa de mejora en seguridad, porque genera una visión de los riesgos de seguridad de la información a lo ancho de la organización, proporcionando una base para mejorar a partir de su estado actual.

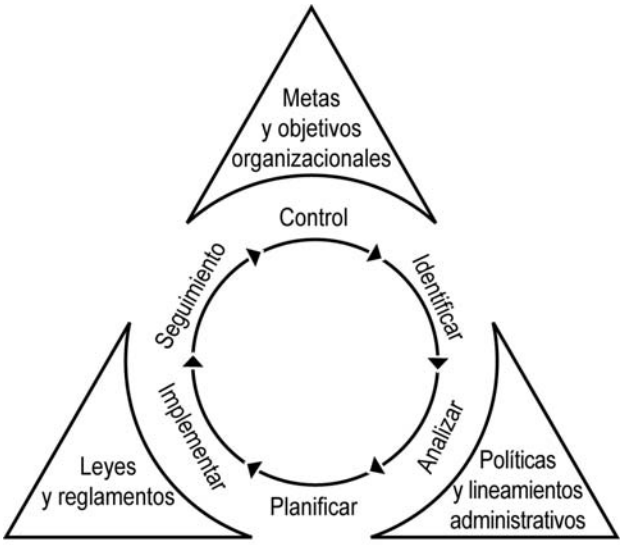

Figura 1-3. Enfoque del manejo del riesgo

El objetivo de OCTAVE es la evaluación del riesgo operacional y se enfoca en temas relativos a la estrategia y prácticas operativas de seguridad implementadas, tal como se muestra en la Figura 1-4, no sólo en la tecnología utilizada. Este enfoque sirve de apoyo a las organizaciones en los procesos de toma de decisiones referentes a la protección de la información basadas en los riesgos operacionales de confidencialidad, integridad y disponibilidad de los bienes relacionados con la información crítica.

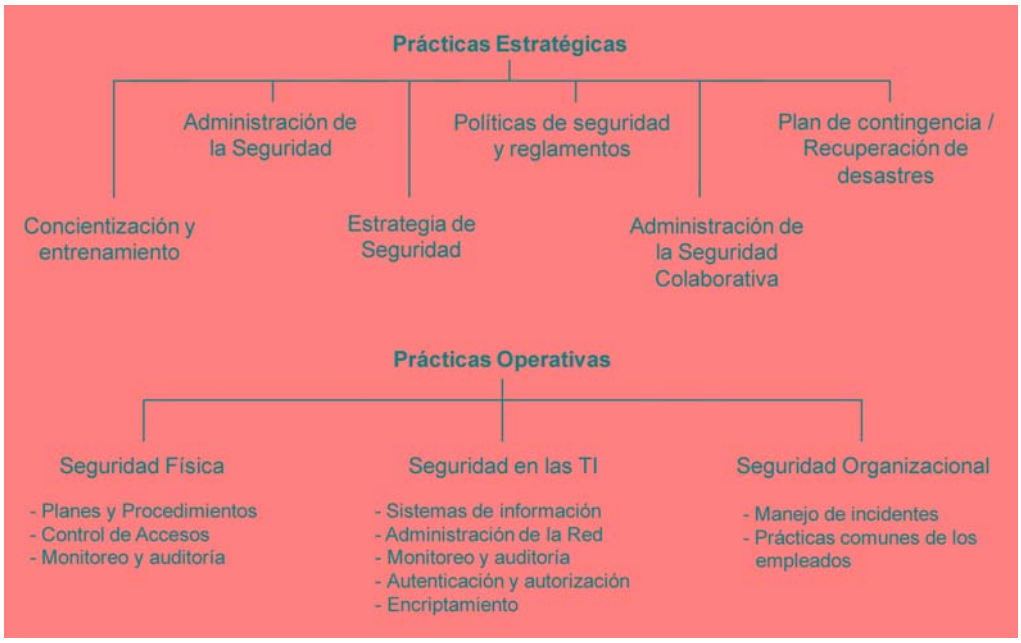

Figura 1-4. Prácticas de seguridad

Una de las particularidades de OCTAVE, es que puede ser realizado por vía de la autogestión; es decir que personal propio de la organización, desde los sectores operativos o de negocios hasta los departamentos de tecnologías de la información (TI), pueden trabajan juntos para determinar las necesidades de seguridad de la organización balanceando los aspectos de riesgo operacional, tecnología y prácticas de seguridad.

La Figura 1-5 nos muestra la forma en que este enfoque analiza las amenazas, así como las fases en que se implementa la seguridad requerida.

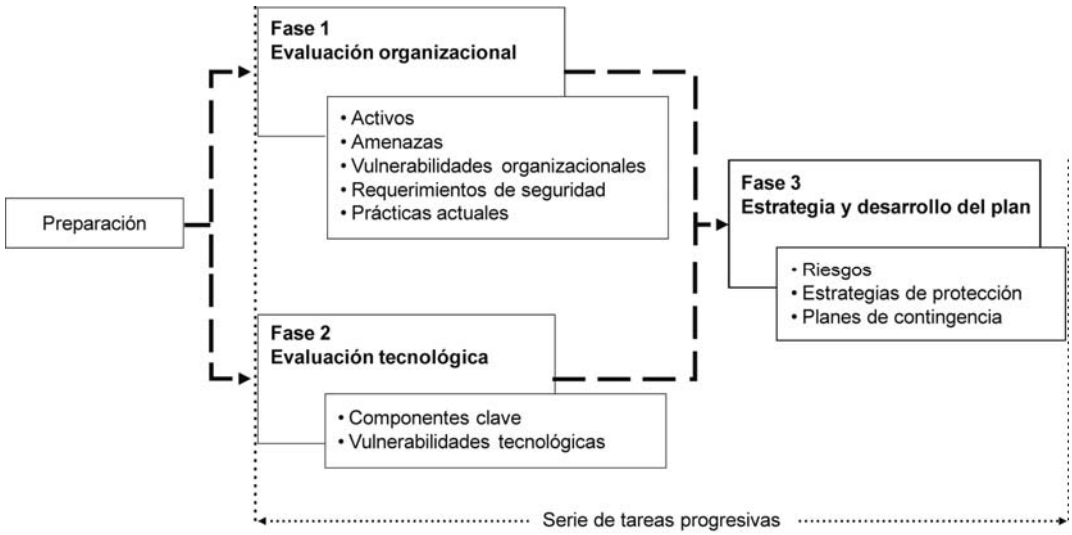

Figura 1-5. Fases en el análisis de amenazas

- ***Fase 1. Evaluación Organizacional***. Identificar los activos críticos y las amenazas a las que están expuestos.
    - Activos
    - Amenazas
    - Vulnerabilidades de la organización
    - Requerimientos de Seguridad
    - Prácticas actuales

- ***Fase 2. Evaluación Tecnológica***. Identificar las vulnerabilidades tecnológicas que originan estos riesgos
    - Componentes clave
    - Vulnerabilidades tecnológicas

- ***Fase 3. Estrategia y Desarrollo del Plan***. Desarrollar una estrategia de protección basada en buenas prácticas, así como planes para la mitigación de los riesgos.
    - Evaluación del riesgo
    - Clasificación del riesgo
    - Estrategias de protección
    - Plan de contingencia

1.4 Sistema de Gestión de la Seguridad de la Información (SGSI)

Debido a la gran cantidad de amenazas existentes en cuanto a sistemas de información y a los diversos controles que deben implementarse para su protección, se hace evidente la necesidad de gestionar los riesgos de seguridad de la información.

Para llevar a cabo una adecuada gestión debemos estar conscientes de que los problemas de seguridad no son únicamente de índole tecnológica, ya que también involucra relaciones sociales; que mediante la gestión no vamos a eliminar todos los riesgos existentes, sino que vamos a dar respuesta a ellos de tal manera que no pongan en riesgo nuestros Sistemas de Información, y lo más importante*: la seguridad no es producto, es un proceso en constante adaptación debido a que las nuevas tecnologías introducen nuevas amenazas*.

Un Sistema de Gestión comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Cubre aspectos administrativos, lógicos, físicos, legales, etc.; es independiente de la plataforma tecnológica y mecanismos concretos que se utilicen.

Podemos afirmar que **la seguridad no es un producto, es un proceso**, por lo cual debe ser gestionada. Dentro de esta gestión, se debe contemplar la mejora continua del sistema, ya que todo evoluciona, especialmente la (*in*)seguridad.

1.4.1 Políticas de Seguridad

El término Política de Seguridad (PS) se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica, en términos generales, qué está y qué no está permitido en el área de seguridad durante la operación de dicho sistema. Al tratarse de "términos generales", aplicables a situaciones o recursos muy diversos, se hace necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica (Specific Policy Management SPM).

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido[12].

Cualquier política que se quiera implementar debe contemplar seis elementos claves en la seguridad de un sistema informático:

- Disponibilidad
  Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

- Utilidad
  Los recursos del sistema y la información manejada en el mismo deben ser útil para alguna función.

- Integridad
  La información del sistema debe estar disponible tal y como se almacenó por un agente autorizado.

- Autenticidad
  El sistema debe ser capaz de verificar la identidad de los usuarios, y los usuarios la del sistema.

- Confidencialidad
  La información sólo podrá estar disponible para agentes autorizados, especialmente su propietario.

- Posesión
  Los propietarios de un sistema deben de ser capaces de controlarlo en todo momento; perder este control a favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de los usuarios.

Para cubrir de forma adecuada los elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política generalmente se divide en puntos más concretos a veces llamados *normativas*.

1.4.2 Seguridad Ligada al Personal

Este tipo de seguridad es una de las más delicadas, ya que existen factores que no pueden ser medidos ni controlados de manera específica.

La falta de conciencia, errores, omisiones o falta de cuidado para con la información que se maneja así como con las instalaciones usadas por parte de empleados, visitantes y cualquier persona vinculada con la organización es un factor de riesgo que puede generar un incidente de inseguridad.

Los empleados permanentes y subcontratados poseen acceso a los datos de las organizaciones a todos los niveles, por lo que esto constituye una amenaza latente.

Un factor de riesgo que durante el último lustro ha surgido es la denomina *ingeniería social,* la cual se refiere a todo artilugio, treta y técnica bastante elaboradas a través de las cuales se engaña a las personas para revelar contraseñas u otra información asociada a la organización o su personal[12]; es utilizada para obtener información confidencial de un sistema de información a través de personas relacionadas con ella mediante métodos no lícitos; básicamente se trata de engaños, cuyo método puede tener un carácter externo o interno al propio sistema de información o infraestructura de comunicaciones, siendo por ello más complejo que la obtención de información a través de las debilidades propias de la implementación y mantenimiento de un sistema.

Los ataques se han vuelto cada vez más difíciles de detectar y valorar a tiempo. Cuando se produce un ataque es difícil de detectar a tiempo, delimitar sus efectos y distinguirlo de simples incidentes o accidentes sin intencionalidad de hacer daño.

1.4.3 Gestión de la seguridad según el Estándar BS 7799-2

La seguridad se gestiona mediante un modelo denominado DPCA (Plan – Do - Check - Act) [12]: Planificar, Hacer, Verificar y Actuar. Este modelo se ejecuta de manera cíclica y siempre mejorando los resultados de la etapa anterior, como se muestra en la Figura 1-6.

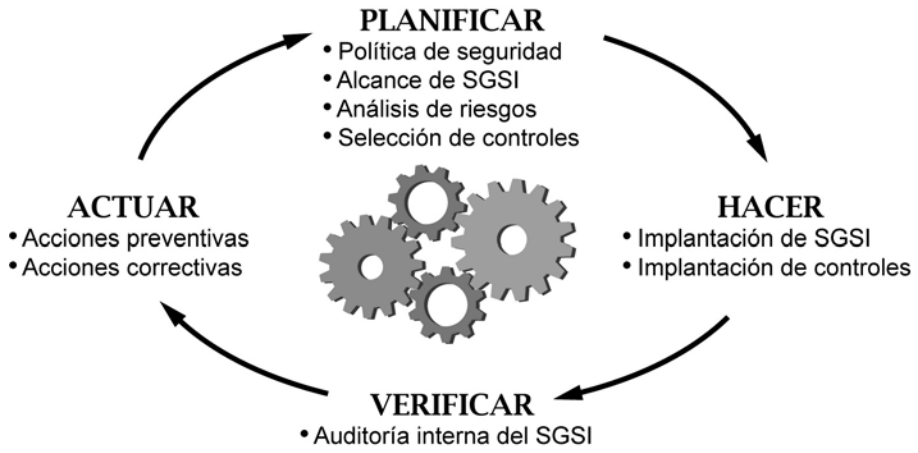

Figura 1-6. Modelo PDCA (Plan – Do – Check – Act)

- **Planificar**
  Se deben responder básicamente las siguientes preguntas para definir el Plan de Acción
  ¿Cuál es el estado actual de la seguridad?
  ¿Cuál es el estado al cual se desea llegar?
  ¿Cómo se quiere llegar a ese estado objetivo?

  Para responder estar peguntas debemos considerar la(s) política(s) de seguridad con que actualmente se cuenta, se debe realizar un análisis de riesgos actuales y futuros, y se deben seleccionar los controles a implementar.
  Un aspecto crítico para esta etapa es la implicación de todos los niveles jerárquicos de la organización.

- **Hacer**
  El hacer implica la implantación del SGSI y la explotación del mismo. En este sentido, se debe realizar la implantación de controles, tanto técnicos como no técnicos y realizar el control de los mismos a fin de determinar su eficacia.

- **Verificar**
  Es necesario verificar la conveniencia, adecuación y eficacia del SGSI dentro de la organización.

  Se deben incluir indicadores de rendimiento a fin de mediar la eficacia y eficiencia del SGSI (¿Mucho?, ¿Poco?, ¿A veces?, ¿Demasiado? . . .)

  De igual manera, se deben realizar los siguientes cuestionamientos:
  ¿Se ajusta a lo deseado?
  ¿Ha sido implantado y se mantiene y ejecuta correctamente?
  ¿Existen nuevos riesgos?
  ¿Hay cambios que puedan afectar al SGSI?

- **Actuar**
  La organización debe mejorar de manera continua la eficacia del SGSI:
  - Revisión de objetivos de seguridad
  - Indicadores de eficacia de los procesos
  - Auditoria periódica y revisiones de seguridad

Es necesario tomar acciones correctivas para eliminar la causa de las no conformidades en la implantación, operación y uso del SGSI, además de las acciones preventivas para eliminar las fuentes de no conformidades potenciales, previniendo su ocurrencia.

Una vez cubiertas todas las etapas del modelo, existe un siguiente paso: la ***certificación***. Este proceso lo debe realizar un tercero y debe indicarse claramente los beneficios que aporta para

- la propia organización
- los inversionistas
- los clientes
- los empleados

1.4.4 Estructura de la gestión de la seguridad

Para cada Política de Seguridad que se defina se debe cubrir su alcance, los procesos y procedimientos a implementar (qué hacer, quién lo debe hacer, cuándo lo debe hacer), las tareas y actividades específicas a realizar así como la forma de realizar (instrucciones técnicas, mecanismos de comprobación, formularios de evaluación, etc.), tal como lo muestra la Figura 1-7.

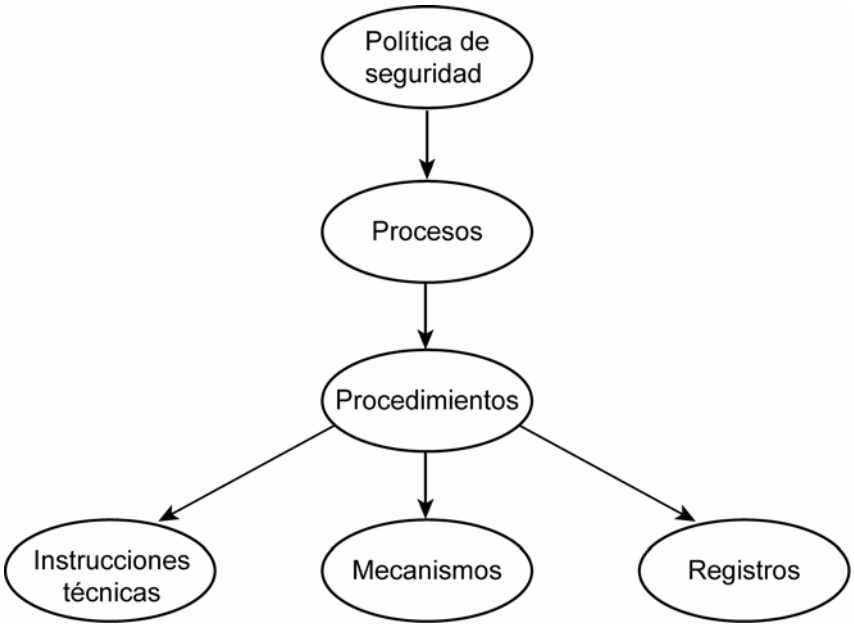

Figura 1-7. Estructura de la Gestión de Seguridad

Finalmente, se deben proporcionar las pruebas objetivas del cumplimiento con las exigencias del SGSI (registros, soporte documental).

1.5 Servicios de seguridad

Una vez revisados los estándares de seguridad podemos decir que un sistema se puede definir como seguro cuando cuenta con las siguientes cuatro características[3]:

1.5.1 Confidencialidad o privacidad

Propiedad o requerimiento de la seguridad que exige que la información sea accedida por cada usuario con base en lo que debe ver en razón a su área del negocio.

1.5.2 Autenticidad

Propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (Verdadero/falso); esta propiedad es especialmente importante en sistemas económicos como la banca, comercio electrónico, bolsa de valores, apuestas, etc.). También es conocida como irrefutabilidad, no rechazo o no repudio ya que se debe conocer en cualquier momento quiénes son los actores que participan en una transacción o una comunicación y no puedan negarlo.

1.5.3 Integridad

Tiene que ver con la protección que se da a los activos informáticos para que solo puedan ser modificados por las personas autorizadas: Escritura, Modificación de información, cambio de estatus, borrado y creación. Esta característica es diferente para cada binomio empleado-organización.

1.5.4 Disponibilidad

Es la garantía de que la información será accedida por los usuarios a través de los servicios de la red según su perfil en el momento requerido y sin degradaciones, donde perfil se entiende como el ámbito de acción que requiere cada empleado para su desempeño laboral en la organización.

Otros requerimientos de seguridad son:

- ***Consistencia:*** Este es un requerimiento que típicamente se solicita a las aplicaciones (aunque no es el único) y consiste en que siempre se comporten igual; es decir que una aplicación siempre tenga el mismo comportamiento ante un evento específico y no que algunas veces cuando se presente el evento se comporte de una manera y en otro momento, ante el mismo evento, se comporte de manera distinta.
- ***Registro:*** Este requerimiento se refiera a que toda acción dentro de un sistema informático (aplicaciones, redes, computadores, etc.) debe dejar un rastro escrito, es decir que se pueda saber lo que se hace dentro del sistema y quién lo hace.

1.6 Arquitectura de la Seguridad

El documento de ISO que describe el Modelo de Referencia OSI, presenta en su Parte 2 una Arquitectura de Seguridad. Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes servicios de seguridad:

1. *Autenticación de entidad par*. Este servicio corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra.

2. *Control de acceso*. Este servicio se utiliza para evitar el uso no autorizado de recursos.
3. *Confidencialidad de datos*. Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.
4. *Integridad de datos*. Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.
5. *No repudio*. Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación.

   Puede ser de dos tipos:
   - *Prueba de origen*. Cuando el destinatario tiene prueba del origen de los datos.
   - *Prueba de entrega*. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del Modelo de Referencia OSI los siguientes mecanismos de seguridad[3]:

- ***Cifrado***. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones. El mecanismo de cifrado soporta el servicio de confidencialidad de datos al tiempo que actúa como complemento de otros mecanismos de seguridad.

- ***Firma digital***. Se puede definir la firma digital como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

La firma digital descrita por ITU y OSI en el entorno de autenticación del directorio utiliza un esquema criptográfico asimétrico. Esta firma consiste en una cadena que contiene el resultado de cifrar con RSA aplicando la clave privada del firmante, una versión comprimida, mediante una función hash unidireccional y libre de colisiones, del texto a firmar.

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera entidad, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

- ***Control de acceso***. Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo. El mecanismo de control de acceso soporta el servicio de control de acceso.

- ***Integridad de datos***. Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad. Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

Existen dos grados en el mecanismo de autenticación:

1. ***Autentificación simple***. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.

2. ***Autentificación fuerte***. Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública. Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación.

La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado. Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario.

El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par.

1.6.1 Roles de seguridad

Dentro de la seguridad informática se pueden identificar básicamente cuatro roles dentro del proceso de seguridad [13]:

- **Administrador de seguridad**: Es la persona encargada dentro de una organización de analizar, diseñar, desarrollar, implantar, probar y mejorar los mecanismos de seguridad que se requieren para proteger los activos informáticos de dicha organización. Es el responsable de que la seguridad sea efectiva y de realizar permanentemente revisiones de la misma en pro de su mejoramiento continuo. El trabajo que realiza en algunas ocasiones lo hace con el apoyo de consultores o asesores de apoyo y con un grupo de expertos en seguridad a su cargo dentro de la organización

- **Auditor, asesor, consultor**: Son generalmente personas externas a la organización que realizan revisiones a la seguridad implantada y realizan recomendaciones para su mejoramiento. Son personas de apoyo para el administrador de seguridad porque le pueden dar consejos de implantaciones de seguridad, hacerlo caer en la cuenta de carencias de seguridad y apoyarlo en nuevos diseños e implantaciones al respecto

- **Forense**: Son expertos que se encargan de realizar análisis de siniestros de seguridad ocurridos dentro de la organización para determinar lo que paso y quién lo hizo, y si es el caso, aportar en procesos penales contra los atacantes

- **Atacante**: Son las personas que buscan tener acceso ilegal a los activos informáticos de una organización. En este rol se pueden distinguir tres tipos:

    - Hacker: Son personas expertas en sistemas que saben de seguridad que lo que buscan es tener acceso a recursos informáticos generalmente con el fin de demostrarse a si mismo y a otros que lo pudieron hacer y conseguir prestigio como expertos en seguridad.
    - Cracker: Son igualmente personas expertas en sistemas y que saben de seguridad y buscan tener acceso a los recursos informáticos con el objetivo de hacer daño a las organizaciones y obtener algún tipo de recompensa, por ejemplo robar datos de una empresa para vendérsela a la competencia, desprestigiar a la organización, robar dinero, etc.
    - Lamers: Esta es una nueva categoría, se trata de personas que no saben mucho de los sistemas de seguridad y se dedican a utilizar herramientas o aplicaciones desarrolladas por otros (hackers o crackers) para hacer daño a las organizaciones. Los lamers no saben de la técnica que hay detrás de un ataque o un mecanismo de violación de un sistema, solo siguen instrucciones respecto al uso de algunas herramientas y realizan fechorías con esto. Este tipo de atacantes puede hacerlo por el simple placer de hacerlo o con ánimo de obtener alguna retribución por sus acciones

1.6.2 Momentos en la implementación de seguridad informática

En lo referente a la seguridad informática, se pueden pensar en tres momentos diferentes para implementarla, los cuales no son excluyentes sino por el contrario complementarios y en la mayoría de las ocasiones dependientes de los recursos que la organización destine para el tema de protección y disponibilidad de la información[14]. Estos momentos son:

- ***Prevenir (Antes)***
  Consiste en evitar que un ataque tenga éxito, a esta categoría pertenecen todas las acciones que se realicen en la organización tendientes a no permitir que ocurra un incidente de seguridad. Ejemplo de esto son los mecanismos de autenticación de usuarios ante un sistema, estos mecanismos pretender evitar que accedan al sistema usuarios no permitidos mediante el uso de técnicas de usuario/clave, biométrico, tarjetas inteligentes, etc.

- ***Detectar (Durante)***
  Ahora, cuando "no es posible o no se desea" prevenir un ataque, es posible que lo que se busque sea darse cuenta de que está recibiendo un ataque durante el mismo momento en el que se está presentado, en este caso lo que se desea es detectar el ataque para así tomar acciones al respecto. Ejemplo de esto son los bloqueos de cuenta de usuario cuando se han realizado intentos ilegales de acceso, digamos 3 intentos errados, después de este número de intentos se bloquea la cuenta porque se presume que hay un atacante que está tratando de acceder al sistema.
  Una precisión que se puede hacer es que no siempre es posible prevenir un ataque, por lo que se debe esperar a que este suceda para tomar acciones al respecto o también se puede dar el caso en el que las herramientas de detección para un ataque o tipo de ataque en particular son muy costosas y la organización decide que sólo se tomará acción sobre el hecho cuando este ocurra y no de manera preventiva; a esto se le llama arreglar sobre la falla.

- ***Recuperar (Después)***
  La tercera y última alternativa es recuperar, en este caso, ya que se ha realizado el ataque y éste ha terminado. Ahora lo que se debe realizar es una revisión de lo que aconteció y tratar de poner en producción nuevamente todos los sistemas afectados, para lo cual se cuenta con dos alternativas:
    - Parar el ataque (evitar que continúe) y entrar a reparar cualquier daño causado por el ataque .
    - Continuar la operación normal e ir defendiéndose del ataque conforme este suceda.

1.6.3 Errores u omisiones en la seguridad

Los errores en la seguridad informática se deben básicamente a la confianza que llegan a tener los usuarios respecto a las herramientas de protección con que cuentan. Sin embargo no sólo se debe tener herramientas de protección, sino que deben ser configuradas de forma particular para cada equipo considerando el grado de confidencialidad de la información almacenada así como del uso que se le da al equipo.

En Internet, los huecos de seguridad más conocidos actualmente son los denominados Cross-Site Scripting (XSS), que aparecen en el 70% de los sitios, mientras que cada vez están más de moda los llamados Cross-Site Request Forgery (CSRF), cuyo uso está creciendo entre la comunidad hacker y cracker. Estos mecanismos son complejos de detectar y erradicar, e implican una amenaza real para muchos sitios web.

Estos errores u omisiones, que en ocasiones son realmente una vulnerabilidad del sistema, deben ser considerados y erradicados para eliminar el mayor número de riesgos posibles en los sistemas de información, ya que cualquier atacante podría aprovecharlos para introducirse y controlar, no sólo el equipo, sino los datos almacenados.

A fin de determinar el grado de confianza de los usuarios debemos revisar las siguientes afirmaciones, las cuales podemos considerar como erróneas [12] y [W7]:

1. *Mi antivirus está al día, así que no puede entrar ningún virus.*
   En general los programas antivirus por sí solos no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas formas que pudieran aparecer conforme las computadoras aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea aún más afectada.
   Aún cuando se tenga actualizado, los antivirus no son infalibles ni sirven para detectar otras amenazas, como el phishing y el spyware.

2. *Uso dos antivirus a la vez, por lo que estoy doblemente protegido.*
   Si un solo antivirus no es suficiente, tampoco lo serán dos; además, pueden interferirse mutuamente y degradar el desempeño del equipo. Si bien las actualizaciones de los antivirus ayudan a proteger, éstos no son infalibles.

3. *Tengo un firewall, así que no corro peligro.*
   Esto únicamente proporciona una limitada capacidad de respuesta, ya que el firewall fiscaliza lo que entra y sale de la PC desde y hacia Internet, pero si no está correctamente configurado puede cometer errores u omisiones que son aprovechados por los piratas informáticos.
   Debido a que las formas de infectarse en una red son múltiples, donde unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones internas (de las que no protege), contar con usuarios con altos privilegios para realizar conexiones implica altos riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el *spoofing*.

4. *Mi sistema o equipo de cómputo no es importante para un craker, por lo que no corro peligro.*
   Hoy día cualquier equipo de cómputo puede ser utilizado como elemento de ataque hacia equipos de terceros: si el pirata consigue, por medio de un virus, controlar a más de un equipo para que intenten conectarse simultáneamente con un sitio Web, éste caerá debido a la demandas de conexiones; además, cualquier PC puede usarse para enviar spam, phishing y otros virus.

Por otro lado, si liberamos o trabajamos con sistemas conectados a la red que no cuentan con claves de acceso se está facilitando el acceso a los datos a cualquier persona. No olvidemos que la mayor parte de los ataques provienen del interior de la propia organización, por lo que se debe proteger todo sistema y equipo de cómputo que almacene información sensible de la organización.

5. *Mi respaldo está al día, así que si pasa algo, puedo restaurar el sistema.*
   Este es uno de los mitos más difundidos y no siempre ciertos, ya que un respaldo puede contener un virus no identificado, por lo que también deben implementarse procedimientos específicos que mantengan libre de contagio los respaldos institucionales que se realicen y así facilitar realmente la continuidad del negocio en caso de emergencia.

6. *Nunca dejo mi dirección de correo en ningún sitio ni estoy registrado en páginas Web, así que es imposible que me roben mi cuenta.T*
   Esto es completamente falso. Por cuestiones de funcionamiento de los navegadores, se guarda esta información en la computadora de uso y en las computadoras de las personas con las que intercambia mensajes. Esta es una puerta que utilizan los virus y sitios maliciosos para extraer una dirección de allí.

Existen otros escenarios que no nos dejan muchas oportunidades para estar a salvo de cualquier ataque cibernético, y que si no se ha establecido un procedimiento adecuado para su manejo es muy probable que perdamos muchos recursos involucrados.

7. *Después de que se infectó el equipo, reinstalé el sistema operativo.*
   Si se reinstala Windows sin dar formato al disco duro, es muy probable que el virus continúe; lo mismo sucede si se formatea y se reinicia, ya que algunos virus residen en la RAM, por lo que se debe apagar por completo el equipo.
   El problema de dar formato es que luego se tiene que invertir tiempo en instalar todas las aplicaciones comerciales, aplicaciones propietarias y reestablecer la información que se tenía mediante un respaldo seguro previamente hecho; con estas acciones estamos evitando que el virus pueda sobrevivir en el equipo.

8. *Si tengo todas las actualizaciones del Sistema Operativo que manejo no existe riesgo alguno.*
   El mantener actualizado el sistema operativo con versiones y parches del mismos son una gran medida de seguridad, sin embargo al igual que con el firewall y el antivirus no es suficiente.
   No todos los ataques se producen por medio de errores del sistema o están dirigidos al kernel del S.O., ya que si alguna de las aplicaciones web (PHP, Perl, etc.) está desactualizada, un ataque sobre algún script de la(s) aplicación(es) puede permitir que el atacante abra una shell y ejecute algún comando de sistema.

9. *No uso Outlook Express ni Internet Explorer, así que estoy a salvo.*
   Si bien es cierto que estos programas son de los más atacados, no son los únicos. La mayoría de los virus infectarán las PC independientemente del software que se utilice para manejar el correo electrónico o bajar archivos de la Web.

10. *No abro ningún archivo adjunto, por lo que los virus no pueden entrar.*
    Este uno de los mayores mitos en la red. Existen virus que ingresan a la PC por el simple hecho de estar conectadas a Internet, si el antivirus no está debidamente actualizado; existen otros que realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

2. Inseguridad de la infraestructura de comunicaciones en las organizaciones

2.1. Entorno general

Las telecomunicaciones han influido de manera directa en el crecimiento de las economías, tanto en los países desarrollados como en los que están en vías de desarrollo ya que se han constituido como una tecnología facilitadora, complementaria y de soporte a un sinnúmero de industrias de bienes de capital, de consumo y de servicios.

Debido a la importancia que ha venido ganando este tipo de infraestructuras, también se han convertido en blanco de diversos ataques, ya sea internos o externos, tales como inexperiencia, mal uso de las aplicaciones, empleados disgustados, accidentes de mantenimiento, virus, delincuencia informática, desastres naturales (inundaciones, incendios, terremotos) o competidores.

La protección de la infraestructura de telecomunicaciones y de la información es una necesidad que se ha tenido desde hace tiempo y se puede decir que en todos los sectores con infraestructuras críticas deben existir planes de protección y seguridad frente a las intrusiones, ataques físicos e incluso catástrofes naturales a fin de asegurar los activos de la organización y permitir la continuidad en su funcionamiento.

Los activos son los elementos que la seguridad informática tiene como objetivo proteger y se encuentran agrupados en tres grandes grupos:

- *Información.* Es el objeto de mayor valor para una organización. El objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre almacenada (algún medio electrónico o físico).
- *Infraestructura.* Software, hardware e instalaciones físicas de la organización, tanto internas como externas.
- *Usuarios.* Individuos que utilizan la infraestructura tecnológica y de comunicaciones que maneja la información.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena o mediante los cuales se transporta. Estas técnicas de aseguramiento las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permitan el acceso a las personas autorizadas para hacerlo.

Para la implementación de estas técnicas de aseguramiento se debe considerar que tanto en las computadoras como en las redes se deben preservar los tres requerimientos de seguridad básicos:

- *Confidencialidad.* Requiere que la información almacenada en un sistema informático pueda ser accesada únicamente por personal autorizado.

- *Integridad*. Requiere que los recursos del sistema informático sólo puedan ser modificados por personal o entidades autorizadas y de una manera controlada.
- *Disponibilidad*. Requiere que los recursos del sistema informático estén disponibles a entidades autorizadas.

Una vez considerados estos requerimiento, y hecha la programación y el configuración de un dispositivo de almacenamiento (o transmisión) de la información a fin de considerarlos seguros, todavía deben ser incluidas las circunstancias no informáticas que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la *redundancia* (en el caso de los datos) y la *descentralización* (en el caso de las comunicaciones).

2.2. Modelo TCP/IP

En [15] se hace una breve descripción de las bases en que se fundamenta el diseño de la familia de protocolos TCP/IP (Transfer Control Protocol/Internet Protocol) y de los ataques potenciales a que están expuestos.

Para que se realice la conectividad entre redes se utiliza la familia de protocolos TCP/IP, ya que son protocolos ampliamente difundidos que permiten la interconexión en la capa de red de manera independiente al Sistema Operativo, lo que los hace a su vez independientes del tipo de la topología de la red.

La familia de protocolos TCP/IP surgió alrededor de 1960 como inicio de un sistema de comunicación basado en redes de conmutación de paquetes desarrollado por el gobierno estadounidense y la agencia de defensa ARPA. Fueron diseñados en principio para funcionar en diferentes medios de comunicación: LANs de Ethernet y Token Ring, incluso en líneas telefónicas ordinarias al permitir la comunicación entre módems.

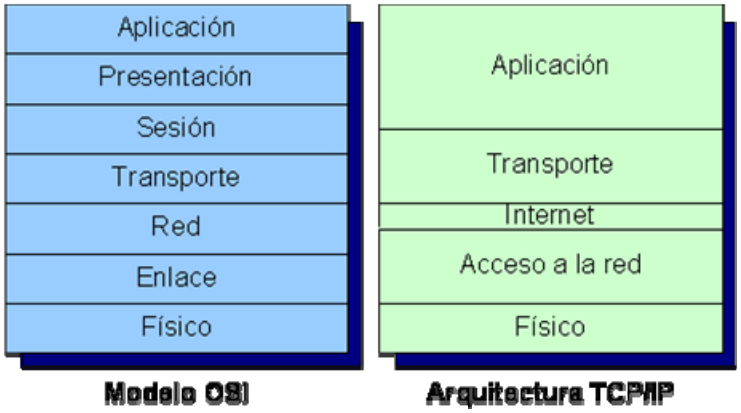

Figura 2-1. Modelo OSI y Arquitectura TCP/IP

Dentro de los equipos que poseen una implementación de la pila de protocolos TCP/IP, se distinguen de forma más detallada dos grupos, todos ellos objetivos de potenciales ataques:

- *Dispositivos de red*. Son los encargados de que tráfico de red fluya dentro o entre redes, por tanto engloban a los repetidores, puentes o bridges, concentradores o hubs, conmutadores o switches, encaminadotes o routers, cortafuegos o firewalls, servidores de terminales y acceso (RAS – Rapid Access Server) que contienen un conjunto de módems o accesos RDSI, y dispositivos de almacenamiento, principalmente.

- *Sistemas*. Equipos que engloban tanto a los clientes de un servicio o comunicación, ya sean PCs o estaciones de trabajo, así como dispositivos móviles (PDAs – Personal Digital Assistant, teléfonos móviles, ...) y a los servidores que proporcionan el servicio. Estos últimos serán el principal objetivo de los atacantes al contener información relevante.

Desde el punto de vista de la seguridad, la familia de protocolos TCP/IP puede ser vulnerada en base a dos conceptos inherentes a su diseño:

1. El formato de los paquetes de los diferentes protocolos.
   Además de la propia información transportada, la información contenida en cada uno de los campos de las cabeceras de los protocolos proporciona una fuente muy valiosa de conocimiento.

2. El modo de funcionamiento de los protocolos.
   Las etapas asociadas a cada proceso de protocolos, así como el método de actuación en las diferentes situaciones posibles, ofrecen la información necesaria para analizar la existencia de vulnerabilidades en la red.

Debido a lo anterior, podemos decir que para realizar el análisis y diseño de una red *segura* es necesario conocer los detalles y características de los protocolos de comunicaciones bajo los cuales opera, mismos que se encargan de transportar la información y datos que se desea distribuir. De igual manera se deben analizar los servicios que se proporcionan en dicha red y sus detalles de funcionamiento a fin de eliminar el mayor número posible de riesgos.

Para implementar un modelo de seguridad aceptable se deben contemplar tres conceptos básicos:

1. *Amenazas a la seguridad*. Acción o serie de acciones que compromete la seguridad de la información propia de la organización.

2. *Mecanismos de seguridad*. Mecanismo de seguridad designado para detectar, prevenir o recuperar el estado de la red ante atentados a la seguridad.

3. *Servicios de seguridad*. Servicio de comunicación que aumenta la seguridad del sistema de procesamientos de datos de una organización y de la información transmitida.

2.3. Vulnerabilidades y Amenazas genéricas

Algunos expertos en el área indican que más del 70 por ciento de los ataques y violaciones a los sistemas de información son realizados por personal interno, esto debido a que conocen los procesos, metodologías de trabajo y, sobre todo, tienen acceso a información sensible de la organización.

Un factor importante a tomar en cuenta es la evolución en el uso de las computadoras y las redes de información, pues sus objetivos han cambiando desde sus inicios: en un inicio sólo se usaban para aplicaciones muy específicas, y en la actualidad se usan para casi toda actividad, aunado a la filosofía de interconexión de equipos con distintas arquitecturas y sistemas operativos generando así gran variedad de datos viajando por la red pudiendo ser accedidos, o interceptados, desde casi cualquier parte del mundo.

2.3.1. Vulnerabilidad

Aunque se puede creer que Riesgo y Vulnerabilidad se podrían englobar un mismo concepto, existe gran diferencia entre ambos, ya que la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de la familia de protocolos TCP/IP (confidencialidad, integridad y disponibilidad de la información)

2.3.1.1. Definición

Una vulnerabilidad es un estado en un sistema de cómputo o un grupo de sistemas que[12]:

- permite que un atacante ejecute órdenes como si fuera otro usuario.
- permite que un atacante tenga acceso a la información restringida.
- permite a un atacante hacerse pasar por otra entidad.
- permite que un atacante genere una denegación de servicio.

El MITRE[1] cree que cuando un ataque se hace posible por una debilidad o una política de seguridad inapropiada, es mejor denominarla "*exposición*".

Una exposición es un estado en un sistema de cómputo (o grupo de sistemas) que no es una vulnerabilidad, pero:

- Permite que un atacante reúna información sobre las actividades del sistema.
- Permite que un atacante disimule sus actividades.

[1] MITRE Corporation, maneja tres centros federales de investigación y desarrollo y un centro dedicado a la seguridad nacional en Estados Unidos patrocinados por el gobierno para apoyar sus misiones cruciales

- Incluye una función que se comporta como se espera, pero puede ser fácilmente puesta en peligro.
- Es un punto primario de entrada que un atacante puede intentar usar para obtener acceso al sistema o a los datos.
- Es considerado un problema de acuerdo a alguna política de seguridad razonable.

Cuando se trata de obtener acceso no autorizado al sistema, un intruso usualmente realiza primero un escaneo de rutina, o investigación del blanco, reúne cualquier dato "expuesto" y luego explota las debilidades o vulnerabilidades de los esquemas de protección con que cuenta el sistema, si es que existen.

Debido al peligro que representan, las vulnerabilidades y exposiciones son aspectos importantes que deben ser considerados cuando se asegura un sistema contra accesos no autorizados.

2.3.1.2. Tipos de vulnerabilidad

Las vulnerabilidades pueden clasificarse según dos criterios[15]; para sus nombres se emplea el término inglés para nombrar la vulnerabilidad, ya que es la forma en que comúnmente se les conoce (Tabla 2-1). Estos criterios son:

- Número de paquetes a emplear en el ataque:
  - *Atomic:* se requiere un solo paquete para llevarla a cabo.
  - *Composite:* son necesarios múltiples paquetes.

- Información necesaria para llevar a cabo el ataque:
  - *Context:* se requiere únicamente información de la cabecera del protocolo.
  - *Content:* es necesario también el campo de datos o payload.

Paquetes / Información	Atomic	Composite
Context	Ping of death Land attack WinNuke	Port scan SYN Flood TCP hijacking
Content	DNS attack Proxied RPC IIS attack	SMTP attacks String matches Sniffing

Tabla 2-1. Tipos de Vulnerabilidades

2.3.1.3. Fuentes de Vulnerabilidades

Para identificar las vulnerabilidades de una red, se debe realizar un análisis de tráfico a fin de compararlo con firmas de ataques conocidos o comportamientos sospechosos y determinar el grado de seguridad con que cuenta la red.

Actualmente se consideran tres leyes imperantes en la seguridad informática[16]:

1. Todo software tiene bugs[2]
2. Todo software de seguridad tiene bugs de seguridad
3. Si el software no es utilizado, no se sabrá qué bugs tiene realmente.

De esto se desprende que entre más se conozca el comportamiento, configuración y servicios proporcionados por la red menos riesgos de seguridad se podrán tener, y que lo que realmente se persigue al hacer un análisis no sólo es comprobar el grado de seguridad de la red, sino el nivel de inseguridad de la misma.

A continuación se presentan las principales fuentes de vulnerabilidad del sistema que permiten una violación a la seguridad [5], [12] y [15].

a) Barrido de puertos

Una de las primeras acciones a realizar para asegurar el sistema es encontrar qué puertos están abiertos dado que se desea conocer qué servicios se están prestando en la red, y en particular en algún servidor.

Cuando un intruso intenta ganar control de un equipo de cómputo o servidor lo que se intenta es aprovechar una debilidad de un servicio o aplicación que se este ejecutando en el sistema y que adicionalmente tenga accesos a la red. Regularmente lo que se busca es lograr un Buffer overflow y finalmente inyectar un código que le permita obtener accesos privilegiados.

El escaneo de puertos es la primera etapa que todo atacante intentará para lograr el control del sistema, sin embargo con esta acción no es posible lograr una evaluación adecuada de los servicios de red debido a que hoy día los programas de defensa (IPS – Instrusion Prevention System, IDS – Intrusión Detection System o Firewall) detectan los programas de escaneo de puertos, aunque con ello no se logra una completa protección ya que existen dos alternativas de ataque adicionales:

- La primera consiste en ir directamente al puerto con un ataque específico. Esta aproximación tiene una gran desventaja, ya que cuando se intenta hacer este tipo de ataques se debe conocer de manera previa la existencia de un servicio específico. Otra desventaja en esta técnica es que no se puede garantizar que no existan programas o dispositivos IPS o IDS en el camino, por lo que el ataque no siempre será exitoso.

[2] Se denomina bug a un error en un programa o en un equipo. Sólo se puede hablar de un bug cuando se trata de un error de diseño, no cuando la falla es provocada por alguna otra cosa.

- La segunda consiste en la fabricación de paquetes. Esta técnica se basa en la idea de un reconocimiento indirecto del sistema; el reconocimiento indirecto consiste en utilizar una IP de un intermediario para crear un conjunto de paquetes y verificar las ID de respuesta.

El primer paso consiste en determinar si es posible usar al intermediario elegido, esto lo hacemos verificando que el sistema tenga abiertos los puertos deseados al enviar paquetes y detectando la respuesta a estos envíos (leyendo los números de identificación); si enviamos 4 paquetes se espera que los números sean continuos y crecientes en el rango. Si estas condiciones se cumplen quiere decir que el intermediario es útil. De no ser así deberemos buscar otro sistema.

Como segundo paso generamos los paquetes con la IP de origen falsificada (la IP del intermediario) cuyo destino es el objetivo de nuestra auditoria o scanner. Se envían los paquetes y finalmente verificamos los números de identificación del servidor intermediario y evaluamos si se incrementaron; de ser así, podemos estar seguros de que el puerto está abierto en el sistema objetivo.

Como puede verse el scanner es muy efectivo y no requiere la realización de exposición directa del origen, además se podrán detectar los puertos sin necesidad de despertar alarmas en los objetivos, dado que existen muchos sistemas relativamente fáciles de usar como intermediarios y en los logs el registro será a sistemas anónimos o terceros no relacionados con este procedimiento. En la mayoría de los casos este ataque pasará inadvertido por el sistema objetivo y nuestra IP no se verá comprometida ni registrada en ningún punto.

b) Identificación de Firewalls

El término firewall proviene de épocas pasadas, aunque el concepto sigue siendo aplicable: entre los edificios de unidades departamentales se construían paredes de ladrillo, de tal manera que si había un incendio éste no se propagaba de un edificio a otro. A estas paredes se les llamó firewalls (barreras de seguridad).

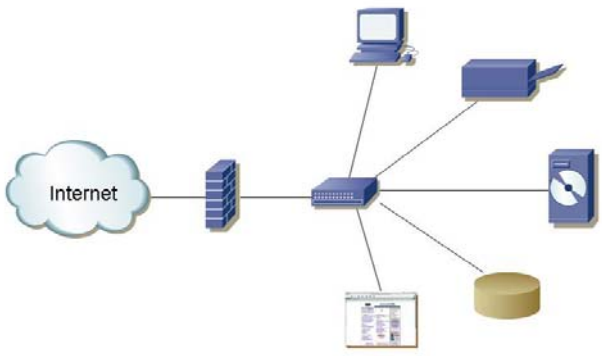

Figura 2-2. Concepto de Firewall

La diferencia entre un firewall tradicional y un firewall informático es que mientras los primeros nos protegen de una amenaza concreta que no ha cambiado a lo largo de la historia (el fuego), los segundos tienen que defendernos de una gran variedad de amenazas (gusanos, ataques de negación de servicio, barrido de puertos, etc.); además, están continuamente evolucionando para encontrar las debilidades de la red.

Ninguna organización puede darse el lujo de establecer una conexión al Internet, sin colocar una barrera de fuego en el punto de conexión. Actualmente, en organizaciones muy grandes, se ha comenzado a definir perímetros de seguridad que, mediante firewalls, definen y controlan accesos dentro de la misma organización.

Las características más comunes de los firewalls [12] y [15] son las siguientes:

- *Bloqueo del tráfico de entrada basado en la dirección del remitente o del destinatario de los datos*. Ésta es la característica más común de los firewalls.
- *Bloqueo del tráfico saliente basado en la dirección del remitente o del destinatario*. Esta característica es menos común, pero permite, por ejemplo, impedir que los empleados accedan a páginas web inapropiadas.
- *Bloqueo del tráfico basado en el protocolo utilizado*. Esta característica impediría, por ejemplo, dejar pasar el tráfico de correo electrónico o el de transferencia de archivos.
- *Bloqueo del tráfico basado en su contenido*. Los firewalls más avanzados pueden llegar a analizar el contenido de los paquetes de datos y rechazar los que incluyan un contenido determinado. Mediante este sistema se puede impedir el paso de, por ejemplo, virus o contenidos pornográficos.
- *Gestión de los recursos internos*. Aunque la principal finalidad de un firewalls es controlar el tráfico de entrada y salida de la red privada, también se podrá configurar para que impida a determinados usuarios internos acceder a recursos internos concretos. Por ejemplo, si se dispone de un servidor Web, se puede restringir su acceso desde la red interna, mientras que se permite desde Internet.
- *Gestión de las direcciones IP privadas*. La dirección IP es lo que permite poder acceder a una computadora. El firewalls puede ocultar las direcciones IP privadas utilizadas por los equipos protegidos y mostrar a Internet exclusivamente una dirección IP pública configurada para el propio firewall.
- *Gestión de red privada virtual*. Una red privada virtual o VPN (Virtual Private Network) es un sistema mediante el cual se puede establecer una conexión segura entre dos puntos de Internet. Algunos firewall incluyen la funcionalidad VPN, con lo que permiten establecer conexiones seguras entre la propia red privada y cualquier computadora conectada a Internet.
- *Caché de datos*. Una misma página Web o unos mismos datos pueden ser solicitados por distintos usuarios de la red interna del firewall. Para aumentar la velocidad de respuesta, el firewall puede guardar una copia de los datos más solicitados en un espacio de memoria intermedia y facilitárselos directamente al solicitante sin tener que completar el acceso a Internet para cada una de las peticiones.
- *Informe de actividad del firewall*. Además de controlar el tráfico, es importante registrar su actividad. Esto permite saber cosas como: datos sobre el intruso que intenta acceder a la red o qué empleado intenta acceder a lugares inapropiados de Internet. El registro de la actividad de un firewall es imprescindible para analizar un posible agujero de seguridad y

actuar en consecuencia. La mayoría de los firewalls incluyen mecanismos para generar informes.

- *Balance de cargas*. En el caso de redes pequeñas es habitual contar con un único punto de acceso. Esta situación es ideal desde el punto de vista de la seguridad, pero no lo es tanto desde el punto de vista de la disponibilidad. Para evitar esto, las redes que necesitan una garantía de disponibilidad cuentan con más de un punto de acceso, y cada uno de estos puntos cuenta con su correspondiente firewall. Bajo este esquema, los distintos firewalls pueden cooperar entre sí haciendo una distribución del tráfico.

Aunque la instalación y configuración de un firewall parece una solución completa, existen muchas otras actividades relacionadas con la seguridad de las que el firewall no nos puede proteger. Por ejemplo, un firewall no puede proteger de:

- *Ataques internos*. Los equipos internos de una red ya están dentro del firewall, por tanto, un firewall no puede hacer nada para frenar los ataques llevados a cabo por cualquier personal, propio o ajeno, desde estos equipos.
- *La ingeniería social*. Este término describe los ataques en los que el pirata obtiene información contactando con los usuarios de la red interna haciéndose pasar por un compañero de trabajo, una persona de mantenimiento o alguien del propio departamento de informática. De esta forma pueden conseguir datos importantes como el nombre de los servidores, direcciones IP o, incluso, las claves de acceso.
- *Virus y caballos de Troya*. Un firewall puede detectar determinados virus rastreando el tráfico de la red. Sin embargo, un firewall no puede impedir el paso de un virus cuando éste viene camuflageado dentro de otro archivo. Mediante un caballo de Troya se puede hacer que su creador reciba todas las pulsaciones de teclas que haga el usuario cuando el programa detecte que se trata de una clave o de los códigos de una tarjeta de crédito.
- *Administradores inexpertos de firewall*. Los firewalls, por sí mismos, no conocen lo que es y lo que no aceptable dentro de una red, a menos que se lo indique el administrador. Los administradores experimentados saben configurar las reglas correctas para bloquear el tráfico inapropiado, pero el personal inexperto puede incluir reglas inútiles que no logran protección alguna. Administrar un firewall de carácter personal es más simple, pero administrar un firewall corporativo requiere que se esté continuamente atento, instalar todas las nuevas actualizaciones del fabricante y analizar los archivos de registro de actividad.

Generalmente se trabaja con dos tipos de Firewall:

1. *Firewall de capa de red*.- Funciona en la capa de red de la pila de protocolos (TCP/IP) como filtro de paquetes IP, no permitiendo que estos pasen a la red interna a menos que se atengan a las reglas definidas por el administrador o las aplicadas por defecto como en algunos sistemas inflexibles de firewall. Una disposición más permisiva podría permitir que cualquier paquete pase el filtro mientras que no cumpla con ninguna regla negativa de rechazo.
2. *Firewall de capa de aplicación*.- Trabaja en el nivel de aplicación; todo el tráfico de HTTP, (u otro protocolo) puede interceptar todos los paquetes que llegan o salen de una aplicación y se bloquean otros paquetes (generalmente sin avisar al remitente). En principio, los

firewall de aplicación pueden evitar que todo el tráfico externo indeseado alcance las máquinas protegidas.

Podemos configurar ad-hoc los firewall de la empresa, pero debemos estar atentos de no dejar ver esta configuración ya que puede ser usada por hackers para entrar al sistema.

c) Proxy

Un Proxy es un sistema de software que permite la conexión de una LAN entera al exterior mediante una sola dirección IP de salida, es decir, si montamos en el servidor principal de la red un módem, tarjeta de red, adaptador RDSI, etc., e instalamos el Proxy (configurando también las aplicaciones cliente en las terminales), todas y cada una de las terminales tendrán acceso al exterior con una sola cuenta de acceso a internet.
Un caso típico para el uso de un proxy es para navegar anónimamente. Al ser el proxy el que accede al servidor web, el proxy puede o no decir quién es el usuario que lo está utilizando. El servidor web puede entonces tener constancia de que lo están accediendo, pero puede que piense que el usuario que lo accede es el propio proxy, en lugar del usuario real que hay detrás del proxy. Existen proxies anónimos y los que sí informan sobre el usuario real que está conectado a través del él.

Utilizar un proxy también tiene sus desventajas, como la posibilidad de recibir contenidos que no están actualizados, tener que gestionar muchas conexiones y convertirse en un cuello de botella, o lo que es pero, el abuso por personas que desean navegar anónimamente. También el proxy puede ser un limitador al no dejar acceder a través suyo a ciertos protocolos o puertos de comunicación.

d) Sistemas Detectores de Intrusos (IDS Intrusion Detection System)

Un Sistema de Detección de Intrusos (IDS) es un programa usado para detectar accesos no autorizados a una computadora o a una red.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red); el IDS detecta, gracias a estos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Existen tres tipos de sistemas de detección de intrusos:

- HIDS (*HostIDS*): un IDS vigilando un solo equipo y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesador es mucho menor.
- NIDS (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.
- DIDS (*DistributedIDS*): sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se pueden fijar reglas de

control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

Los IDS suelen disponer de una base de datos de "firmas" de ataques conocidos. Dichas firmas permiten al IDS distinguir entre el uso normal del equipo y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento de ataque.
En redes es necesario considerar el lugar de colocación del IDS. Si la red está segmentada con hubs (capa 1 del modelo OSI) no hay problema en analizar todo el tráfico de la red realizando una conexión a cualquier puerto. En cambio, si se utiliza un switch (capa 2 del modelo OSI), es necesario conectar el IDS a un puerto SPAN (Switch Port Analiser) para poder analizar todo el tráfico de esta red.

e) Identificación de Sistemas Operativos

En la actualidad, existe gran cantidad de Sistemas Operativos, tales como Windows, HP-UX, Linux, Solaris, etc., y cada uno tiene características propias que lo diferencian de los demás: distintas implementaciones de la pila de protocolos TCP/IP, diferentes comportamientos de envío y conformación de paquetes especialmente formados, distintas respuestas en función del protocolo utilizado (TCP, ICMP, ARP), etc.

Al realizar una revisión de seguridad, auditoría o test de penetración, es importante, antes de empezar a enumerar qué servicios activos existen, reconocer el Sistema Operativo del servidor remoto que se está analizando, ya que el procedimiento, las herramientas y las técnicas a emplear son diferentes. A esto es lo que se le conoce como *Fingerprinting de Sistemas*.

El *Fingerprinting de Sistemas* es la técnica que utilizan la mayoría de analizadores de puertos avanzados para intentar descubrir el sistema operativo de un servidor remoto. Ésta identificación se basa en los tiempos de respuesta a los diferentes paquetes ACK y SYN al establecer una conexión en el protocolo TCP/IP.

Los sistemas operativos incluyen dos vulnerabilidades principales: la configuración por defecto y los errores (bugs) de programación.

Básicamente existen dos formas de intentar descubrir el sistema operativo presente en un servidor remoto: forma activa y forma pasiva[15].

- Forma activa de reconocimiento del Sistema Operativo

La forma de obtener información se realiza mediante herramientas originalmente creadas para solucionar problemas en la red, las cuales se basan en el envío de paquetes al sistema a atacar:

- *traceroute*. Técnica que permite conocer todos los sistemas existentes en un camino entre dos equipos. Se basa en el manejo del campo TTL de la cabecera IP de un paquete, de forma que es capaz de determinar uno a uno los saltos por los que un determinado paquete avanza en la red.
- *fping, gping y Pinger*. Herramientas que permiten obtener la lista de dispositivos IP activos.
- *finger*. Permite identificar el sistema operativo del host mediante una petición del tipo *finger root@host.dominio.com* o *finger –l @ host.dominio.com*

- Forma pasiva de reconocimiento del Sistema Operativo

Estas técnicas, al contrario de las anteriores, se basan en el monitoreo del tráfico asociado al sistema a atacar. En función de los atributos y características de los paquetes, principalmente de las cabeceras TCP, se determina su origen.

- *TTL*. ¿Cuál es el valor del campo Time To Live (TTL) en los paquetes salientes?
- *Tamaño de la ventana*: ¿cuál es el valor fijado por el S.O.?
- *TOS*: ¿Sufija algún valor para el campo Tiempo de Servicio (TOS)?
- *DF*: ¿Se activa o no el bit de no fragmentación?

La forma activa puede ser fácilmente detectable por los IDS debido a que las técnicas de este tipo se basan en el envío de paquetes al sistema objetivo. Las técnicas pasivas, por el contrario, no son detectables fácilmente, salvo mediante la utilización de herramientas de detección de sniffers.

Existe un método alternativo de descubrir qué sistema está presente en la mayoría de los servidores remotos importantes presentes en Internet, sin hacer ningún tipo de ruido ni ninguna prueba complicada al usar NETCRAFT[3], lo cual significa un grave peligro para cualquier infraestructura de telecomunicaciones.

f) Configuración de servicios y servidores

Uno de los mayores problemas a este respecto se basan en la configuración por default de sistemas y aplicaciones, ya que el fabricante no siempre cubre todos los aspectos de seguridad y mucho menos los específicos para la organización que los utiliza.

Se debe tener especial cuidado en configurar los servicios de red de manera que sólo permita la ejecución de acciones específicas y controladas dentro de sí misma.

Lamentablemente, los diferentes servicios que un sistema ofrece se pueden convertir en puertas de entrada al sistema, o en fuentes de ataques hacia otros. Si cada servicio ofrecido es un posible problema para la propia seguridad, pudiera pensarse que lo ideal sería no ofrecer servicios, sin embargo esto no puede ser posible, ya que es necesaria la conectividad entre equipos. Considerando este escenario, se debe habilitar los servicios mínimos necesarios para que todo funcione correctamente; esto choca directamente con las políticas de la mayoría de fabricantes de sistemas Unix, que por defecto mantienen la mayoría de servicios abiertos al instalar un equipo nuevo, por lo que es responsabilidad del administrador preocuparse de cerrar aquellos que no son estrictamente necesarios.

Ejemplos de servicios que suele ser necesario ofrecer son telnet o ftp; que si bien no se pueden negar completamente, sí se puede configurar de manera ad-hoc para que sólo sea posible acceder a ellos desde ciertas máquinas; también es una buena idea sustituir estos servicios por sus equivalentes pero cifrados, como la familia de aplicaciones SSH, además de concienciar a los usuarios para que utilicen estos equivalentes. Debemos recordar siempre - y

[3] NETCRAFT, compañía dedicada básicamente a realizar estadísticas del uso de software en Internet. Dispone de un servicio Web en el que con la simple introducción del nombre del servidor a analizar, en segundos proporciona la información acerca del servidor Web, el Sistema Operativo, etc.

recordar a los usuarios - que cualquier transferencia de información en texto plano entre dos sistemas puede ser fácilmente capturada por herramientas instaladas en una máquina intermedia, con lo simplemente utilizando telnet estamos poniendo en juego la seguridad de sistemas y redes completas.

g) Promiscuidad en redes

Cuando una tarjeta o adaptador de red se configura en modo promiscuo, captura todos los paquetes que pasan por él.

El método más común de captura de tráfico en redes de comunicaciones es a través del uso de *sniffers*. Un *sniffer* es un programa que captura datos de la red; todo lo que pasa por él lo registra y almacena para un análisis posterior. De esta forma, sin necesidad de tener acceso a ningún sistema de la red, se puede obtener información, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves.

Los paquetes de información tienen dos direcciones de destino; la dirección IP y la dirección física o dirección MAC que es única por cada interfaz de red. Cada interfaz de red tiene un filtro de comunicaciones que discrimina los paquetes cuya dirección física de destino no coincide con la dirección física de la interfaz.

Los *sniffers* funcionan por una sencilla razón: en muchos de los protocolos de acceso remoto a las máquinas se transmiten las claves de acceso como texto plano, y por lo tanto, capturando la información que se transmite por la red se puede obtener este tipo de información y el acceso ilegítimo a una determinada máquina, de ahí la peligrosidad de la instalación de un sniffer y más aún, de mantener la red en modo promiscuo.

2.3.2. Amenaza

2.3.2.1. Definición

Una amenaza es un hecho que puede producir daño, un delito o falta en el ámbito del Derecho.

Trasladando esta definición al ámbito informático una amenaza se puede definir como cualquier factor que comprometa al sistema informático o los recursos de la red, el cual puede ser de origen humano, técnico o por desastre natural.

2.3.2.2. Fuentes de amenazas

De manera general, las amenazas pueden provenir de las siguientes fuentes [5] y [12]:

a) Errores de Hardware

Las amenazas en hardware se dan por fallas físicas que presente cualquier elemento de los dispositivos que conforman a la computadora.

Los problemas más identificados para que el suministro de energía falle son el bajo voltaje, ruido electromagnético, distorsión, alto voltaje, variación de frecuencia, etcétera. Aunado a lo anterior encontramos los desperfectos de los equipos, bajo rendimiento, la pérdida de dispositivos físicos por deterioro o incorrecto funcionamiento, pérdida total o parcial del equipo por sobrecalentamiento, problemas con carga estáticas, entre otros.

b) Errores de la red

Un error altamente peligroso es la existencia de puntos de red sin equipos conectados, ya que cualquier persona puede conectar un equipo y utilizar los recursos disponibles.

Otro factor es dejar a la vista y de manera accesible, la infraestructura de conexión, ya que cualquiera puede realizar una desconexión de equipos sin que ésta sea autorizada.

c) Problemas de tipo lógico

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o malicia) en la computadora abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o spyware.

El software instalado en las computadoras y en los equipos configurados para el procesamiento de la información llegan a ser el blanco en la introducción de software malicioso, tales como virus informáticos, worms de red, troyanos y bombas lógicas

Los virus son programas capaces de reproducirse y causar daño. Actualmente, el daño no sólo afecta a los archivos del sistema, sino que se ha expandido a aplicaciones de la familia Office: Word, Excel PowerPoint y Access. Esto se convierte en enormes pérdidas de información y horas-hombre de trabajo.

Otro medio por el cual se puede atentar contra la infraestructura de cómputo es el uso indiscriminado del correo electrónico, ya que genera pérdida de tiempo de los empleados y pone en riesgo a la organización al replicar correos de los que no siempre se verifica su origen.

d) Sinistros

Un siniestro (robo, incendio, inundación): una mala manipulación de archivos o una acción malintencionada derivan en la pérdida del material o de los archivos de información.

Los desastres suelen ser de muchos tipos, tales como rayos, fallas eléctricas o picos de potencia. También se incluye el polvo, la humedad o la temperatura excesiva.

e) Factor Humano

Dentro de este factor podemos mencionar tres grandes grupo:

- El *usuario*: causa del mayor problema ligado a la seguridad de un sistema informático (por que no le importa, no se da cuenta o a propósito).

- El *personal interno* de Sistemas. Las luchas de poder llevan a disociaciones entre los sectores de la organización y en ocasiones a soluciones incompatibles para la seguridad informática.

- Un *delincuente informático*: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.). Los delincuentes informáticos son personas que disponen de conocimientos específicos, cierta experiencia, un buen conjunto de herramientas y, sobre todo, motivación y tiempo. Las modalidades de motivación de un *ciberdelincuente* son muy variadas: reto personal, relevancia social, interés económico, rivalidad, diversión, venganza, etc.

  Julio C. Ardita, director de una empresa de seguridad y exhacker define cuatro tipos de intrusos. "Los tipos de intrusos se pueden caracterizar desde el punto de vista del nivel de conocimiento, formando una pirámide. Estos se clasifican en:

  - **Clase A**
    El 80% en la base de la pirámide son los nuevos intrusos que bajan programas de Internet, están jugando y son pequeños grupitos que se juntan y dicen vamos a probar.

  - **Clase B**
    Es el 12% siguiente, son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen cómo detectar el sistema operativo que está usando la víctima, examinan las vulnerabilidades del mismo e ingresan a través de ellas.

  - **Clase C**
    Corresponde al 5%. Es gente que sabe, conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

  - **Clase D**
    El 3% restante es el pico de la pirámide. Cuando entran a determinados sistemas buscan la información que necesitan.

  Para llegar de la Clase A hasta la D se necesitan en promedio de 4 a 6 años, por el nivel de conocimiento que se requiere asimilar: práctica, conocimiento, programación, tiempo dedicado."

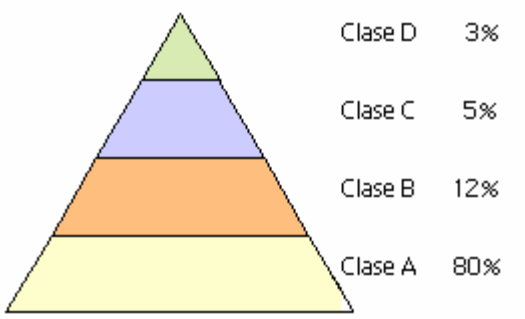

Imagen 2-3. Distribución de Intrusos en la red

Actualmente los hackers han cambiado sus objetivos, ya no buscan la fama, prefieren crear amenazas silenciosas que tarden mucho más en descubrirse y así tener un mayor margen de tiempo para ganar más dinero.

2.3.2.3. Clasificación

Las amenazas intencionadas a las redes de comunicaciones que derivan en algún tipo de modificación o generación de flujo de datos transmitidos pueden ser clasificadas, de manera general, en los siguientes tipos [3] y [5]:

- *Intercepción*. Amenaza a la confidencialidad cuando un elemento no autorizado consigue el acceso a un objeto específico del sistema.
- *Modificación*. Amenaza a la integridad de la transmisión al modificar el elemento interceptado.
- *Fabricación*. Amenaza a la autenticidad al fabricar un objeto similar al original atacado, de forma que es difícil distinguirlos entre sí.
- *Interrupción*. Amenaza a la disponibilidad al hacer que un objeto se pierda, quede inutilizable o no disponible.

2.3.3. Ataques comunes

Al inicio del uso de las computadoras y redes los ataques involucraban poca sofisticación técnica. Los ataques internos se basaban en utilizar permisos para alterar la información almacenada, mientras que los externos se enfocaban en acceder a la red de manera remota simplemente con averiguar una clave válida.

Conforme ha avanzado la tecnología, se han desarrollado formas de ataque cada vez más sofisticadas, lo cual ha permitido tomar el control de sistemas completos, generando con ello grandes pérdidas, ya que entre más alto es el grado de dependencia tecnológica de la organización mayor será el daño ocasionado (daño económico, social o moral).

El desarrollo de nuevas versiones de sistemas operativos y aplicaciones permite eliminar vulnerabilidades conocidas, sin embargo los tipos de ataque también evolucionan y aprovechan nuevas vulnerabilidades, por lo que no basta con protegerse de los ataques conocidos, sino que se debe ir más allá para evitar nuevas formas de ataque.

Un pirata informático no quiere ser descubierto, por lo que procura no dejar rastros de sus ataques, lo que implica para los administradores de redes estar monitoreando el comportamiento de la red a fin de detectar comportamientos fuera de lo común.

De acuerdo con [5], [12] y [15] dentro de los principales ataques encontramos:

a) Robo de identidad (pishing)

El robo de identidad online consiste en realizar acciones utilizando los datos de otra persona. Como lo más normal es que esas acciones sean ilegales (compras online con tarjetas robadas, apertura de cuentas bancarias, etc.) este tipo de ataques suelen tener graves consecuencias para los usuarios que han sido víctima de ellos. Como norma general, se define que ha habido un robo de identidad cuando una persona utiliza la información personal de otra, como nombre, dirección, o número de Seguro Social, para realizar actividades ilegales como abrir cuentas de crédito, sacar dinero del banco o hacer compras.

Este tipo de ataque también se le conoce como pishing, que consiste en atraer mediante engaños a un usuario hacia un sitio web pirata donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y contraseñas de las cuentas bancarias, números de seguridad social, entre otras.

Uno de los métodos más comunes para hacer llegar a la "víctima" a la página falsa es a través de un e-mail en una aparente comunicación oficial electrónica que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que se ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.

Una de las consecuencias más peligrosas de este fraude es que la barra "falsa" queda en memoria aún después de salir de ella pudiendo hacer un seguimiento de todos los sitios que visitamos posteriormente y también el hacker puede espiar todo lo que se envía y recibe a través del navegador mientras se encuentre ativo.

Riesgos del Phishing:

- Los datos facilitados pueden ser empleados por el pirata informático para acceder a las cuentas de los usuarios y gestionar su dinero o realizar compras sin su autorización o consentimiento.
- Puede emplearlos para abrir nuevas cuentas bancarias o tarjetas de créditos en nombre de la *víctima* pero con otra dirección de correo, lo que supone un robo de identidad.
- El equipo de la víctima puede servir para difundir virus programados para hacer llegar los e-mails fraudulentos a más usuarios.

Protección de Datos:

1. Evitar el primer impulso de responder a cualquier e-mail. Leer detenidamente la información ayuda mucho; en muchos casos los hackers los lanzan a modo de spam, por lo que puede llegar a recibir un correo de un servicio del que no se es usuario.
2. No enviar información personal o financiera por Internet; no es el método más seguro. De hacerlo, asegúrese de que lo hace bajo una conexión segura (icono de candado, https, etc...), aunque a veces los hackers también pueden emular esto.
3. Revisar de vez en cuando sus movimientos bancarios para asegurarse de que los cargos en su cuenta son legítimos.
4. Emplear soluciones de seguridad informática actualizadas: antivirus, firewalls, etc... Algunos e-mails fraudulentos instalan programas maliciosos en el equipo, con el consiguiente riesgo de virus, spyware, etc...
5. Tener cuidado con la ejecución de archivos adjuntos o la descarga de éstos desde e-mails o páginas webs; pueden contener virus informáticos, troyanos o keyloggers.
6. Comprobar con el verdadero y "supuesto remitente" del e-mail si ha enviado el correo. Muchas entidades financieras han puesto en funcionamiento teléfonos, e-mails, o webs de contacto para denunciar cualquier intento de phishing en su nombre.

b) Spoofing

Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un hacker simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de *snoofing* o *tampering*. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de e-mails falsos.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza éste para entrar en otro, y en otro. Este proceso, llamado *looping*, tiene la finalidad de desaparecer la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del *looping* es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un *insider*, o por un estudiante a miles de kilómetros de distancia, pero que ha tomado la identidad de otros. El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el *IP spoofing*, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

Otros ataques de falseamiento conocidos son:

- *DNS Spoofing*: En este caso se falsea una dirección IP ante una consulta de resolución de nombre (DNS) o viceversa, resolver con un nombre falso una cierta dirección IP.
- ARP Spoofing: Hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que un determinado equipo de una red local envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
- Web Spoofing: El pirata puede visualizar y modificar una página web (incluso conexiones seguras SSL) solicitada por la víctima.
- E-mail Spoofing: Falsifica la cabecera de un e-mail para que parezca que proviene de un remitente legítimo. El principal protocolo de envío de e-mails, SMTP, no incluye opciones de autenticación, aunque existe una extensión (RFC 2554 [17]) que permite a un cliente SMTP negociar un nivel de seguridad con el servidor de correo.

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema, aunque también es conseguida a través de una simple llamada telefónica.

c) Engaño a firewalls y a Sistemas Detectores de Intrusos

Los Sistemas Detectores de Intrusos (SDI) observan cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las diferentes acciones que integran este proceso se denominan comúnmente patrones o firmas del ataque.

Estas firmas pueden ser simples, como cadenas de caracteres, estructuras de memoria o bits, pero también pueden ser más complejas como vectores o expresiones matemáticas. Una ventaja de este método es que permite centralizar las labores de detección en el conjunto de firmas que posee el SDI, minimizando así, la carga de procesamiento del sistema. Muchos productos comerciales utilizan este enfoque e inclusive periódicamente proporcionan actualizaciones de éstas firmas de tal manera que puedan detectarlas en el menor tiempo posible.

Existen SDI enfocados a la detección de anomalías, los cuales se encuentran constantemente monitoreando el sistema para así detectar cualquier cambio en los patrones de utilización o el comportamiento del mismo. Si algunos de los parámetros monitoreados sale de su regularidad, el sistema generará una alarma que avisará al administrador de la red sobre la detección de una anomalía, sin embargo este tipo de detección es bastante compleja, debido a que la cuantificación de los parámetros a observar no es sencilla y a raíz de esto, se pueden presentar los siguientes inconvenientes, como la generación de falsas alarmas si el ambiente cambia repentinamente, por ejemplo, cambio en el horario de trabajo; de igual manera, un atacante puede ir cambiando lentamente su comportamiento para así engañar al sistema.

Los inconvenientes antes mencionados pueden ser controlados mediante una implementación robusta y minuciosa.

Según el tipo de monitoreo, hay SDI con detección orientada al host o detección orientada a la red.

El *modelo orientado al host* se basa en el monitoreo y análisis de información, que refleja el estado del host donde éste reside. La mayoría de la información que este tipo de sistema recopila es obtenida a través del sistema operativo del host. Esto último causa complicaciones debido a que la información que se procesa no contiene registros del comportamiento, de bajo nivel, de la red.

Los SDI que utilizan *el modelo orientado a la red*, fundamentan su monitoreo en información recolectada de la red. Generalmente, ésta información es capturada mediante mecanismos de sniffing. El *sniffing* consiste en habilitar la interfaz de red en modo promiscuo para que así capture todos los paquetes que reciba, incluso aquellos que no le han sido destinados.
En base al mecanismo antes expuesto, se pueden definir patrones o firmas de ataques, según la estructura, información y ocurrencia de los paquetes.

d) Vulnerabilidad en el software

Un sistema operativo o una aplicación puede ser vulnerable a los ataques de programas maliciosos si es capaz de ejecutar un programa o rutina que no sea parte de sí mismo. Esta condición la cumplen todos los sistemas operativos, muchas aplicaciones de oficina, editores gráficos, sistemas de diseño y otros tipos de paquetes de software que utilizan o permiten el uso de lenguajes *script*.

El crecimiento de vulnerabilidades del software se debe, en principio, al crecimiento sostenido de una variedad de programas maliciosos, especialmente de los elaborados con Java Script y Visual Basic Script.

Las principales razones parecen ser los esfuerzos incesantes de las compañías antivirus por desarrollar nuevas y mejores tecnologías basadas en el análisis heurístico, la emulación de códigos y la virtualización de procesos con el fin de trabajar con archivos ejecutables Win32, mientras que los programas maliciosos basados en scripts se han mantenido fuera de su alcance cuando se trata de un análisis en profundidad y de acciones paliativas. Una segunda razón es el uso activo de los lenguajes script para implementar una serie de vulnerabilidades en navegadores populares de Internet. La penetración en navegadores vulnerables es hoy la táctica más popular usada para expandir programas maliciosos.

e) SQL Injection

La inyección de código SQL es una vulnerabilidad informática que se emplea en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.

Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.

La vulnerabilidad puede ocurrir cuando un programa "arma" descuidadamente una sentencia SQL, con parámetros dados por el usuario, para luego hacer una consulta a una base de datos; al ejecutarse esa consulta, el código SQL inyectado también se ejecutará y podría hacer un

sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos llegando incluso a ejecutar código malicioso.

Es, de hecho, un error que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro, por lo que este tipo de ataques se centra en las aplicaciones desarrolladas sobre ASP.Net y SQL Server, sin embargo también son aplicables a otras bases de datos y plataformas de desarrollo, como MySQL y PHP.

Una de las partes más vulnerables en una página web es la información contenida en la base de datos, y por lo tanto es una de las partes a las que hemos de prestar más atención.

f) Cross Site Scripting (XSS)

Cross Site Scripting (XSS) es el nombre que recibe una vulnerabilidad que afecta no tanto a los servidores como a los usuarios que navegan a páginas de Internet. La causa de la vulnerabilidad radica en la pobre verificación por parte de los sitios web de las cadenas de entrada enviadas por los usuarios a través de formularios, o directamente a través del URL. Estas cadenas, en el caso de ser maliciosas, podrían llegar a contener scripts completos.

El mayor riesgo de este tipo de ataques es que la entrada maliciosa no la proporciona el mismo usuario que ve la página, sino un atacante, que consigue que el script se ejecute en el navegador del usuario. La víctima ejecuta el código de manera indirecta cuando confiadamente hace clic sobre un hiperenlace fraudulento, que puede estar presente en el sitio web del atacante, en un mensaje de correo electrónico o de un grupo de noticias, o en cualquier otro lugar que no levante sospechas. Debido a que en este caso la víctima es el visitante del sitio web y no el propio sitio, este tipo de vulnerabilidades no ha recibido la atención que se merece.

El cross site scripting funciona de la siguiente manera:

1. El usuario sigue un enlace, que incluye codificada una cadena de entrada como argumento de entrada a algún parámetro de la página del sitio web.
2. El sitio web no valida (o lo hace pobremente) la entrada anterior y genera dinámicamente una página HTML que incluye el código introducido en el hiperenlace por el atacante.
3. Este código se ejecuta en el navegador de la víctima, con los mismos privilegios que cualquier otro código legítimo del mismo sitio web.

Esta vulnerabilidad puede estar presente de forma directa (también llamada persistente) o indirecta (también llamada reflejada). Cada una se trata de forma diferente.

> ***Directa***: Este tipo de XSS es el que normalmente es censurado; así que es muy poco común que puedas usar tags como <script> o <iframe>
>
> ***Indirecta***: Esta es un tipo de vulnerabilidad muy común y muy poco explotada. Consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas, sin usar sesiones; sucede cuando hay un mensaje o una ruta en la URL del navegador o en una cookie.

g) Virus y gusanos

Los virus, gusanos y troyanos son programas malintencionados que pueden provocar daños en el equipo y en la información del mismo. También pueden hacer más lento Internet e, incluso, pueden utilizar el equipo infectado para difundirse e infectar equipos conocidos o a toda la red.

Un *virus* es código informático escrito con la intención expresa de replicarse; se adjunta por sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Los virus pueden dañar el software, el hardware y los archivos.

Un *gusano*, al igual que un virus, está diseñado para copiarse de un equipo a otro, pero éste de manera automática. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en el sistema, se propaga sin la intervención del usuario y distribuye copias completas de sí mismo por las redes. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

Cuando se lanzan nuevos gusanos, se propagan muy rápidamente. Bloquean las redes y posiblemente provocan esperas largas (a todos los usuarios) para ver las páginas Web en Internet. El gran peligro de los gusanos es su habilidad para propagarse en grandes números.
Estos ataques se pueden evitar mediante la instalación de programas *antivirus*. Un programa antivirus tiene como principal función el impedir la infección de los equipos de cómputo por parte de toda clase de *malware* (software malicioso) como pueden ser virus, gusanos, troyanos, etc, a través de su vacuna (protección en tiempo real), y de ser el caso buscar, encontrar, desinfectar y/o eliminar cualquier virus que sea encontrado durante el análisis.

Esta protección es fundamental, ya sea que se esté conectado a Internet o no, ya que a través de medios extraíbles como disquetes, CDs, DVDs y/o medios de memoria extraíbles y similares también se pueden contraer infecciones. Un antivirus siempre debe estar actualizado, ya que en caso contrario la protección que proporciona no es del todo completa.

h) Spam

También conocido como *junk-mail* o *correo basura*, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un letargo en la red al ocupar el ancho de banda.

i) Caballos de Troya (Trojanos o back doors)

Esta vulnerabilidad está asociada más a los sistemas de información que a los protocolos TCP/IP; sin embargo también es empleada para introducir servicios TCP/IP no deseados en el sistema destino y así poder ejecutar ataques remotos con posterioridad llegando incluso a tomar por completo el control del sistema.

Este tipo de ataque también es conocido como puertas traseras (*back doors*) y consiste en introducir dentro de un programa una rutina o conjunto de instrucciones no autorizados para que el programa original ejecute acciones no deseadas. En el caso de *trojanos* que afectan a los servicios TCP/IP de manera directa, son programas completos que normalmente se justifican como herramientas de administración remota, típicamente del sistema operativo Windows.

Si es instalada por un hacker, esta herramienta tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar passwords y datos confidenciales y enviarlos vía mail a un equipo remoto.

Hoy en día existen tres grupos principales de comportamientos en la categoría TrojWare:

1. *Backdoor, Trojan-PSW, Trojan -Downloader*. Estos programas son los comportamientos troyanos más expandidos y representan un 75% de la categoría TrojWare (el porcentaje de cada categoría por sí misma supera el 20%).
2. *Trojan, Trojan-Spy*. Estos comportamientos representan casi el 9% de los programas TrojWare y muestran índices promedio de crecimiento. Hay muy pocas posibilidades de que estos comportamientos alcancen el incremento numérico necesario para unirse al primer grupo; asimismo, es poco probable que su número decaiga hasta el nivel del tercer grupo.
3. *Trojan-Proxy, Trojan-Dropper, Trojan-Clicker, Rootkit*. Este grupo de comportamientos cae en un rango del 0.7% al 2.1%. Excepto por *Rootkit*, el índice de crecimiento de los comportamientos en este grupo no sobrepasa el 40%. Los programas Rootkit se unieron a este grupo en 2007 gracias a su rápido índice de crecimiento del 116.1%. Es posible que el número de programas con un comportamiento particular crezca hasta alcanzar el nivel del segundo grupo, aunque es mucho más probable que la proporción de programas maliciosos en este grupo siga decayendo bajo la presión de los integrantes del primer grupo.

Los programas Trojan Spy, que son los más peligrosos para los usuarios, y los más dinámicos en cuanto a su evolución, son programas de familias de códigos maliciosos diseñados para robar datos personales de los usuarios de juegos en línea y de sistemas bancarios.

j) Bombas lógicas

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruya o modifique la información o, peor aún, provoque que el sistema colapse.

k) Ataques a contraseñas

Este tipo de ataque se basa en obtener archivos de contraseñas de sitios para después comprometer cuentas al intentar adivinar las contraseñas. Una vez que el intruso obtiene acceso a una cuenta de usuario, intentan ganar privilegios de Administrador descifrando su contraseña o aprovechándose de alguna vulnerabilidad del sistema.

Estos incidentes apuntan a la necesidad de que los administradores de sistemas deben proteger de manera adecuada a los sistemas de este tipo de ataques. Se recomienda hacer lo siguiente:

- *Proteger el archivo de contraseñas* para que un intruso no pueda obtener una copia del mismo.
- Asegurar que las *contraseñas son robustas* para que no puedan ser descifradas con facilidad, o utilizar una tecnología en la que las contraseñas no estén localizadas en el archivo de contraseñas.
- Asegurar que el sistema está *actualizado con parches de seguridad* y soluciones temporales.
- Observar la *actividad inusual en la red.*

l) Spyware

El spyware son pequeñas aplicaciones cuyo fin es obtener información sin que el usuario se de cuenta y, de manera general, con fines comerciales. Estos programas normalmente se instalan en el equipo tras ejecutar aplicaciones gratuitas en Internet (freeware, shareware, cookies, media players, file sharing), o bien haciendo clic en enlaces que no parecen sospechosos a simple vista, como pueden ser los pop-ups.

Riesgos del Spyware:

- Atentan contra la privacidad del usuario ya que difunden a terceros sus hábitos de navegación.
- En algunos casos modifican la página de inicio por defecto del navegador, o archivos del sistema.
- El spyware provoca, principalmente, una reducción en el rendimiento del sistema, malfuncionamiento de aplicaciones, y cuelgues del sistema.

Recomendaciones Antispyware:

- Prevenir: asegúrese de que los programas que instala no contienen spyware, lea con detenimiento los contratos de licencia (EULA) que suelen aparecer al comienzo del proceso.
- Valore la necesidad que tiene de instalar un determinado programa.
- Instale una herramienta antispyware para bloquear pop-ups y evitar así que instale accidentalmente programas de este tipo.
- En la actualidad existen en Internet multitud de herramientas anti-spyware, gratuitas y comerciales: instale una.

m) Negación de servicio (Denial of Service - DoS)

Se trata de una amenaza diseñada específicamente para impedir el funcionamiento normal de un sistema sobrepasando los límites de recursos establecidos para un servicio determinado, obteniendo como resultado la eliminación temporal del servicio y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados, es decir, agotar de alguna forma los recursos de un equipo como para que no pueda atender las peticiones legítimas. Los destinos de estos ataques suelen ser servidores web o DNS (Domanin Name System), aunque también pueden ser routers o enlaces de red.

En principio estos ataques no representan mayor peligro a los servidores de aplicaciones, ya que no modifican los contenidos de la información ni permite obtener información sensible a la organización; simplemente persiguen entorpecer el acceso de los usuarios a los servicios de un sistema.

Su principal objetivo es asumir el control de una computadora que puede ser controlada de manera remota por intrusos. Si se tiene acceso a los dispositivos de red, éstos pueden reinicializarse o apagarse, con diversos niveles de afectación en la red de comunicaciones de la organización afectada.

La defensa ante los ataque de denegación de servicios no es directa, ya que este tipo de ataque se basa en vulnerabilidades inherentes al diseño del protocolo TCP/IP. Los tres protocolos en los que se basan las técnicas de saturación de paquetes, o *flooding*, son TCP, UDP e ICMP.

Durante los últimos años se ha extendido este tipo de ataques de la plataforma Unix al entorno gráfico Windows. Esto, unido al incremento de conexiones de banda ancha en hogares (tecnologías xDSL y cable) ha incrementado el número de ataques que pueden realizarse. De igual manera, debido a la potencia del ancho de banda del que disponen los routers, éstos están siendo empleados como agentes para originar ataques DoS.

Una variante más potente de los ataques DoS son los DDoS (Distributed Denial of Service), que se basan en realizar ataques DoS de forma masiva a un mismo objetivo desde diferentes puntos en la red, de tal forma que la potencia del ataque sea mayor[15].

El proceso está compuesto de cuatro etapas:

1. *Fase de escaneo*. Se utiliza un conjunto objetivo de sistemas muy elevado, y se prueban frente a una vulnerabilidad conocida.
2. *Obtener acceso a los sistemas*. Se obtiene acceso a parte de esos sistemas a través de la vulnerabilidad.
3. *Instalación de herramientas DDoS*. Se instala la herramienta DDoS en cada sistema comprometido.
4. *Utilización de los sistemas*. Se utilizan estos sistemas para escanear y comprometer nuevos sistemas.

El modo de operación genérico de las herramientas de DDoS tiene la siguiente topología: el intruso se comunica mediante comandos con un elemento denominado handler. Éste se encarga de gestionar el registro, realizado previamente, de un conjunto de agentes, normalmente elevado en número, que son realmente el origen de los paquetes del DDoS. Por tanto, los agentes y el handler conforman una red de ataque, que actúan en el momento en que el handler retransmite a todos y cada uno de los agentes las órdenes invocadas por el intruso remotamente. Originalmente la comunicación entre estos elementos se realizaba por puertos fijos y, a la larga, éstos de volvieron conocidos, por lo que este modo de funcionamiento podía ser detectado por sistemas IDS con facilidad. La difusión en el uso del IRC o chat, ha dado lugar a la utilización de este medio (y sus puertos TCP asociados, del 6660 al 6669) para constituir los canales de control de los elementos de un DDoS.

2.3.4. Factor Humano

El factor humano es una de las fuentes de inseguridad más importante debido a la interacción tan fuerte que mantiene para con cualquier sistema de información, desde el uso de instalaciones hasta el acceso a información confidencial. Es por ello que se debe identificar estos riesgos a fin de implementar controles específicos para eliminar o disminuir dichos riesgos.

2.3.4.1. Ingeniería Social

Se denomina *ingeniería social* (literalmente traducido del inglés, Social Engineering) a todo artilugio, tretas y técnicas bastante elaboradas a través de las cuales se engaña a las personas para conseguir información en torno a los equipos o sistemas de información, tal como contraseñas u otra información, por lo que es más complejo que la obtención de dicha información a través de las debilidades propias de la implementación y mantenimiento de un sistema [12] y [W8]. Como podemos ver, la ingeniería social es utilizada para obtener información confidencial de un sistema a través de las personas mediante métodos no lícitos.

Los métodos son diversos:

- El primero y más obvio es simplemente una demanda directa, donde a un individuo se le pide completar una tarea directamente. Aunque probablemente tenga menor éxito, éste es el método más fácil y el más sincero. El individuo sabe exactamente lo que quiere que haga un tercero.
- El segundo método es ejecutado indirectamente en una situación previamente ideada donde el individuo es simplemente una parte de la misma. El mismo puede ser persuadido porque cree en las razones proporcionadas. Esto involucra mucho más trabajo para la persona que realiza el esfuerzo de la persuasión, y casi ciertamente se involucra obteniendo un conocimiento extenso del "objetivo". Esto no significa que las situaciones no tienen que ser basadas en hecho real. Cuando menos falsedades, mayor la factibilidad de que el individuo en cuestión juegue el papel que le fue designado.

2.3.4.2. Personal disgustado

Los empleados disgustados, al ser parte de la organización y conocer puntos clave de la misma se convierten en una gran amenaza para la misma.

Exploran los errores del sistema operativo o las debilidades de cualquier recurso de cómputo para hacer que éstos fallen o utilizan otros métodos más poderosos para destruir o corromper la información.

2.3.4.3. Piratas informáticos

Un pirata informático, también denominado hacker, es una persona que investiga la tecnología y herramientas tecnológicas de una forma no convencional. Al realizar este tipo de investigación, se

convierten en expertos informáticos que terminan por entrar en lugares donde no estaba previsto que entraran y violan la seguridad de algunos sistemas. La definición más popular que se tiene de hacker es: *persona que viola los sistemas de cómputo*.

Existen, fundamentalmente, dos tipos de expertos informáticos:

- Los que ven Internet coma un media para satisfacer su ego. Estas personas fijan sus retos personales en lograr entrar a sitios prohibidos; probar que saben más que los demás, que son más poderosos.
- Los que claramente buscan un lucro o beneficio personal. Para este tipo de personas, Internet se ha vuelto una herramienta más de la delincuencia. En esta categoría entran, desde los que simplemente pretenden hacer usa de unos recursos de forma gratuita, hasta los que se dedican al espionaje o sabotaje industrial.

En ambos casos, se trata de personas que no les importa realizar actividades ilícitas, porque piensan, que nunca se les va a atrapar. Alrededor de la piratería informática existe todo un mundo de términos que, de alguna forma, clasifica a los piratas dependiendo de su nivel de experiencia o de sus verdaderas intenciones. Los medios de comunicación en inglés utilizan de forma general el término hacker (literalmente rompedor) para referirse a lo que en español llamamos pirata informático. No obstante, dentro de la comunidad hacker se realizan verdaderos esfuerzos para que la sociedad diferencie a un hacker, un pirata bueno, de un cracker, un pirata malo.

Los distintos términos que se manejan hoy en día dentro de la piratería son los siguientes [5], [12] y [15]:

a) Hacker

Según su propia definición, un hacker es una persona que posee conocimientos y habilidades especiales en el uso de la informática y disfruta resolviendo retos técnicos. Estas personas tienen unos profundos conocimientos sobré programación, redes de cómputo y sistemas de seguridad, lo cual incluye habilidades para traspasar las protecciones de las redes.
No existe un titulo oficial de hacker, sino que es algo que se adquiere al demostrar elevados conocimientos informáticos y practicar dos principios básicos: compartir sus conocimientos y no cometer actos ilegales. De hecho, con la compartición de sus conocimientos con el resto de la comunidad hacker es como demuestra sus habilidades. En cualquier caso, la idea es que ningún problema se tenga que resolver por segunda vez. Los verdaderos hackers piensan que la información debe ser gratuita y tienen como uno de sus objetivos el que esto sea así.
A los hackers con mucha experiencia y reputación mundial se les conoce como *demigod*.

b) Cracker

Los crackers son una especie de *hackers* que no respetan sus buenos principios. Se caracterizan por esforzarse en resaltar su capacidad para romper los sistemas de seguridad, lo que les lleva a crear descontrol para atraer la atención de los medios de comunicación. Curiosamente, ellos mismos se denominan hackers, y la prensa también se refiere a ellos con esta denominación. También se denomina cracker a la persona que desprotege un programa comercial para que pueda ser utilizado libremente. En esta línea, un crack es el proceso o clave necesario para realizar la desprotección del programa.

c) Samurai
Se trata de un hacker que ofrece sus servicios para realizar una labor legal. Frecuentemente son contratados para auditar los sistemas de seguridad de las redes de las empresas.

d) Whacker
Se trata de una persona que comparte la filosofía de un hacker, pero que no llega a tener sus habilidades. Es algo así coma un hacker principiante. Claro que, si está en sus comienzos, entonces recibe el nombre de *larva, lamer o newbie*. Incluso, para los más novatos, el nombre asignado es el de *wanabee* (una forma coloquial de escribir Want to be, "quiere ser") o *sript kiddie* (aprendiz de programador). La inexperiencia hace que cualquier principiante sea muy peligroso, aunque no tenga malas intenciones. Hay quien llama *lamer* a los novatos de cracker y *newbie* a los novatos de hacker.

e) Lamer
Este grupo es quizás el más numeroso por los miembros que posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es una computadora, pero su uso y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en un sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro equipo, le fascinan enormemente.
Este es quizás el grupo que más peligro representa en la red ya que ponen en práctica todo el Software de Hackeo que encuentran en la red. También emplean de forma habitual programas sniffers para controlar la red, interceptan contraseñas y correo electrónico y después envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada más.

f) Copyhackers
Es una nueva clasificación sólo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura de códigos y después se los venden a los bucaneros, personajes que serán detallados más adelante.
Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo.
La principal motivación de estos personajes es el dinero.

g) Bucaneros
Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "crackeados" pasan a denominarse "piratas informáticos", por lo que el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

h) Phreaker

Este grupo es bien conocido en la red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas de prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo es en estos últimos tiempos cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta, ya que se emplea la informática para su procesamiento de datos.

i) Newbie

Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de hacking y descubre que existe un área de descarga de buenos programas de hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

j) Script Kiddie

Denominados Skid kiddie o Script kiddie, son el último eslabón de los clanes de la Red.

Se trata de simples usuarios de Internet, sin conocimientos sobre Hackeo o el Crackeo en su estado puro; en realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red; en realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los archivos Readme de cada aplicación. Con esta acción, activan algún virus, o infectan su propia computadora.

Esta forma de actuar es la de total desconocimiento del tema, lo que le lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los "pulsabotones" de la Red. Los Kiddies en realidad no son útiles en el progreso del Hacking.

2.4. Estadísticas de amenazas y vulnerabilidades básicas

El recoger datos de un número razonablemente grande de sistemas y agruparlos por tipo, fuente y destino, permite elaborar estadísticas sobre los ataques más comunes, las áreas más seguras (o inseguras) y la forma en que las preferencias de determinado grupo de exploits cambian en el tiempo.

En la Tabla 2-2 se muestra la lista de las vulnerabilidades más utilizadas realizada por el proyecto Smallpot [W9] para septiembre del 2004:

Vulnerabilidad	Frecuencia
Sasser worm FTPD Server buffer overflow	290
Mydoom.A Backdoor execute exploit	260
Microsoft SQL Server SQ password brute-force guessing	84
Dameware remote buffer overflow	64

Microsoft Knowledge Base Q313418 null password vulnerability	50
MS03-026 RPC Vulnerability	13
MS02-061 Elevation of Privilege in SQL Server	7
Mydoom. A Backdoor execute command	7
MS01-059 Unchecked Buffer in Universal Plug and Play service	4

Tabla 2-2. Vulnerabilidades más frecuentes de acuerdo con Smallpot (septiembre de 2004)

Cada año, el Instituto SANS (SysAdmin, Audit, Network, Security) y el NIPC (Infrastructure Protection Center, United State National), junto con el FBI elaboran una lista de las vulnerabilidades de seguridad más críticas en Internet.

a) SANS

De acuerdo con el SANS, la Tabla 2-3 nos muestra las vulnerabilidades principales del 2004 para el sistema operativo Windows, y en la Tabla 2-4 se muestran las correspondientes a Linux.

Principales vulnerabilidades de los sistemas Windows
W1 Servidores y Servicios Web
W2 Servicio de estación de trabajo
W3 Servicios de Acceso Remoto de Windows
W4 Microsoft SQL Server (MSSQL)
W5 Autenticación
W6 Navegadores web
W7 Aplicaciones de archivos compartidos
W8 Exposiciones LSAS
W9 Clientes de correo
W10 Mensajes Instantáneos

Tabla 2-3. Vulnerabilidades del S.O. Windows en 2004

Principales vulnerabilidades de los sistemas UNIX
U1 Sistema de Nombre de Dominio BIND (Berkley Internet Name Domain)
U2 Servidor Web
U3 Autenticación
U4 Sistemas de control de versiones
U5 Servicio de Transporte de Correo
U6 Protocolo de Dirección Simple en la Red (SNMP)
U7 Open Secure Sockets Layer (SSL)
U8 Configuración deficiente de Servicios de Empresas de NIS/NFS
U9 Bases de datos
U10 Kernel

Tabla 2-4. Vulnerabilidades del S.O. LINUX en 2004

b) Kaspersky Lab

Kaspersky Lab, en su boletín de seguridad 2007[W10] nos presenta un análisis de la evolución de los programas maliciosos o malware, de los programas publicitarios o adware y de los programas potencialmente maliciosos en 2007, así como la forma en que han evolucionado desde 2006.

A continuación se presenta un resumen de los mismos.

Casi todas las epidemias en 2007 fueron de corta duración y se limitaron a regiones y países específicos en vez de expandirse abiertamente por Internet. Esta tendencia se ha consolidado como el estándar de facto en la organización de epidemias.

Sin duda, Storm Worm (aka Zhelatin en el sistema de clasificación de Kaspersky Lab) sobresale entre los nuevos programas nocivos en 2007. Este gusano salió a la luz en enero de 2007. Durante todo el año, mostró una amplia variedad de comportamientos, métodos de interacción entre sus componentes, métodos de expansión y tácticas de ingeniería social, y llevó a los expertos antivirus al límite en su intento de mantenerse al ritmo de las últimas creaciones de los autores desconocidos.

Zhelatin fue la manifestación de casi todos los logros de los métodos de los autores de virus en los últimos años, muchos de los cuales habían aparecido previamente, como prueba de código de concepto. Estos incluían tecnologías rootkit, códigos basura y botnets capaces de autoprotegerse contra análisis y estudios, y de interactuar entre ordenadores infectados a través de redes P2P (Peer To Peer), sin necesidad de un centro de control. El gusano utilizó todos los modos disponibles para expandirse, desde los tradicionales (correo electrónico y sistemas de mensajería instantánea) hasta los servicios ofrecidos en la era de la Web 2.0 (redes sociales, blogs, foros y servicios RSS). Los ciberdelincuentes también aprovecharon el creciente interés de los usuarios de Internet en los servicios de video, camuflageando a Zhelatin como un archivo de video.

La función principal de Storm Worm era crear redes para la posterior organización de envíos masivos de correo spam y el lanzamiento de ataques DoS. En cuanto a los ataques DoS, se convirtieron en uno de los temas clave de la seguridad informática en 2007.

Tras haber tenido un uso activo en 2003-2004, los ataques DoS no se constituyeron en una herramienta de particular preferencia entre los delincuentes cibernéticos sino hasta 2007. En el 2008 regresaron, aunque no tanto como una herramienta para sacar dinero a sus víctimas, sino como un medio de librar batallas políticas y competitivas. La historia del ataque librado contra Estonia en mayo de 2007 logró amplia cobertura mediática, y muchos expertos lo consideran el primer evento de la ciberguerra. Resultó claro que los competidores comerciales de las víctimas estaban en el trasfondo de los ataques DoS en 2007. Sólo cuatro años antes, los ataques DoS servían como armas en manos exclusivamente de piratas extorsionadores y de usuarios maliciosos. Sin embargo, hoy en día, se han convertido más bien en un producto para el envío de correo spam y de malware elaborado según especificaciones de los clientes. Los servicios de anuncios para los ataques DoS se han vuelto algo común, y los precios se comparan ahora con los de envíos organizados de correo spam.

En 2007, los negocios de los ciberdelincuentes produjeron nuevas formas de actividad delictiva. El negocio de los programas maliciosos desarrollados a pedido del cliente creció e incluso se

comenzó a ofrecer apoyo técnico a sus clientes. Quizás el ejemplo más claro de esta línea de negocios es el del programa espía troyano Pinch. Los autores crearon más de 4,000 variantes de este troyano en el transcurso de varios años; la mayoría de estas variaciones se hicieron a pedido de otros usuarios maliciosos. Parece que esta historia llegó a su fin en diciembre de 2007, cuando el jefe del Servicio Federal de Seguridad de Rusia anunció que ya se conocían las identidades de los autores de Pinch.

Otro ejemplo similar tiene que ver con el virus Fujack. Esta maliciosa creación china tenía el propósito de robar datos de los usuarios de juegos en línea y sus autores la vendían a cualquiera que lo solicitara. Existen ahora varios cientos de variantes de Fujack. El autor de Fujack ganó casi 12,000US$, al menos esa fue la suma anunciada por las autoridades chinas, quienes al final lograron arrestar al ciberdelincuente junto con varios de sus clientes.

Fujack fue uno de los más notorios programas maliciosos de las familias de troyanos para juegos en 2007. En 2006, los troyanos bancarios (diseñados para robar datos de cuentas bancarias) llegaron a dominar el escenario, y Kaspersky Lab predijo que 2007 sería testigo de la competencia entre troyanos bancarios y de juegos en cuanto al número de nuevos programas.

En términos cualitativos, los resultados de fin de año de 2007 muestran que los troyanos de juegos ganaron ampliamente: el número de troyanos de juegos excedió al de los troyanos bancarios. Es importante remarcar que aún no hay una competencia directa entre estas dos familias de troyanos ya que sus públicos objetivo son distintos. Esto se confirma con el hecho de que todavía no hemos visto ningún troyano de juegos capaz de robar datos de una cuenta bancaria. Mientras que en teoría sería simple crear esta clase de híbrido, esta función no resulta importante ni atractiva para los autores de virus.

Los más importantes eventos de 2007 incluyen los ataques masivos a sitios web y la posterior inserción de programas maliciosos (o vínculos a sitios infectados) en los sitios web cautivos. Uno de estos eventos fue el ataque a casi 10,000 sitios italianos en junio, cuando la serie de vulnerabilidades conocida como MPack se insertó en los sitios Web atacados. Este tipo de ataques perversos también se dio alrededor del mundo durante todo el 2007. El mayor de estos ataques se produjo a fines de ese año cuando más de 70,000 sitios web en diferentes países se infectaron con un código malicioso expandido por otro troyano de juegos.

El incidente italiano del Mpack llamó la atención de otra operación delictiva: durante las investigaciones se estableció que el programa malicioso se había insertado en los sitios Web de la Red Rusa de Negocios (RRN). Un detallado análisis concluyó que se utilizó la RRN como plataforma para distribuir docenas de programas maliciosos cientos de veces. Las discusiones se orientaron hacia el así llamado hospedaje a prueba de balas. Los proveedores de este servicio garantizaban el anonimato de sus clientes, la protección contra investigaciones legales y la ausencia de todo archivo de registros.

Estalló un gran escándalo alrededor de la RRN que se prolongó durante el verano y parte del otoño de 2007 hasta que la RRN se desvaneció en las sombras tras errar por diferentes plataformas de hospedaje en diferentes países alrededor del mundo, en lo que fue un esfuerzo por minimizar la verdadera magnitud de sus operaciones.

En la Tabla 2-5 se presentan algunos datos de este estudio.

Porcentaje Total	2007	2006	Crecimiento
TrojWare	201958	91911	119.73 %
VirWare	12416	6282	97.64 %
MalWare	5798	4558	27.20 %
AdWare	14382	2583	456.79 %
RiskWare	2690		
Total	237244	105334	125.23 %

Tabla 2-5. Programas nuevos en 2006 y 2007

2.5. Métodos de protección

Analizando la seguridad de las redes, no está de más reflexionar sobre el comentario expuesto por Bruce Schneier en el foreword de la segunda edición de Hacking Exponed: "si una red de ordenadores tiene una vulnerabilidad de seguridad, pero nadie la conoce, ¿es insegura?"; concluyendo que "una red de ordenadores con una vulnerabilidad de seguridad es insegura para aquellos que la conocen. Si nadie la conoce – porque sea una vulnerabilidad que no ha sido descubierta- entonces la red es segura. Si una persona la conoce, entonces la red es insegura para él, pero segura para cualquier otro. Si el fabricante del equipamiento de la red la conoce, si los grupos de investigación de seguridad la conocen, si la comunidad kacker la conoce … - la inseguridad de la red aumenta a medida que las noticias sobre la vulnerabilidad salen a la luz" [12].

Aunque se observa claramente una evolución en la tendencia del malware y los ataques informáticos, también las herramientas de protección a los sistemas de información e infraestructura tecnológica de las organizaciones han sufrido evoluciones y grandes avances, es por ello que deben ser considerados en cualquier esfuerzo de protección.

Para llevar a cabo una adecuada implementación y administración de la seguridad debemos estar conscientes de que los problemas de seguridad no son únicamente tecnológicos, ya que también involucra relaciones sociales; que mediante la gestión de seguridad no vamos a eliminar todos los riesgos existentes, sino que vamos a dar respuesta a ellos de tal manera que no se pongan en riesgo nuestros sistemas de información, y lo más importante*: la seguridad no es un producto, es un proceso en constante adaptación debido a que las nuevas tecnologías introducen nuevas amenazas*.

Existe un viejo dicho en la seguridad informática que dice: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida. Los medios para conseguir una protección son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no les correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en, y por, el procedimiento elegido.

- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves de acceso distintas y permisos bien establecidos e identificables, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Mantener un registro de las actividades realizadas por los empleados dentro de cada uno de los sistemas de información.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

De los anterior se desprende que un modelo de seguridad a implementar debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red.

Podemos considerar que estas capas son:

- Políticas de seguridad de la organización
- Auditoria
- Sistemas de Seguridad a nivel Router-Firewall
- Sistemas de Detección de Intrusos
- Plan de respuesta a incidentes
- Pruebas de Penetración (Penetration test).

Un modelo de seguridad tiene que ser adaptable y variable, es decir debe permitir que se le eliminen y agreguen ciertos elementos sin comprometer los requerimientos de seguridad en su totalidad; así mismo se puede implementar un esquema de seguridad sin modificar la topología de red que una organización estaba empleando previamente.

3. Protección y Prevención

Hoy día no podemos hablar de un sistema de información cien por ciento seguro debido al desarrollo de nuevas tecnologías de la información, y al uso que de ellas se hace, tanto en beneficio como en perjuicio de entidades e individuos.

A fin de contrarrestar las amenazas y vulnerabilidades a las que está expuesta una organización se debe definir el desarrollo e implementación de niveles de seguridad para cualquier sistema de información. Esto se puede realizar mediante el apoyo de las denominadas Políticas de Seguridad Informática (PSI), cuyo objetivo es generar una concientización, respeto y aplicación de métodos de operación por parte del personal involucrado a través de un marco normativo que establece la solución de seguridad para cada aspecto de las organizaciones.

El propósito fundamental de crear una arquitectura de seguridad mediante la implementación de PSI es asegurar que la estrategia de negocio y la seguridad en las tecnologías de la información están articuladas. Al establecer una PSI dentro de la organización se puede controlar un conjunto de vulnerabilidades mediante un nivel específico de protección, aunque no se logre la seguridad total.

La Figura 3-1 nos muestra una analogía de la evolución del hombre con la evolución de la seguridad en las infraestructuras de comunicaciones. Si bien no existe una metodología que proteja de manera total a los sistemas de información e infraestructura asociada, sí se puede definir el ámbito de protección sobre plataformas, procedimientos administrativos y/o de operación mediante las PSI, así como la estrategia a seguir.

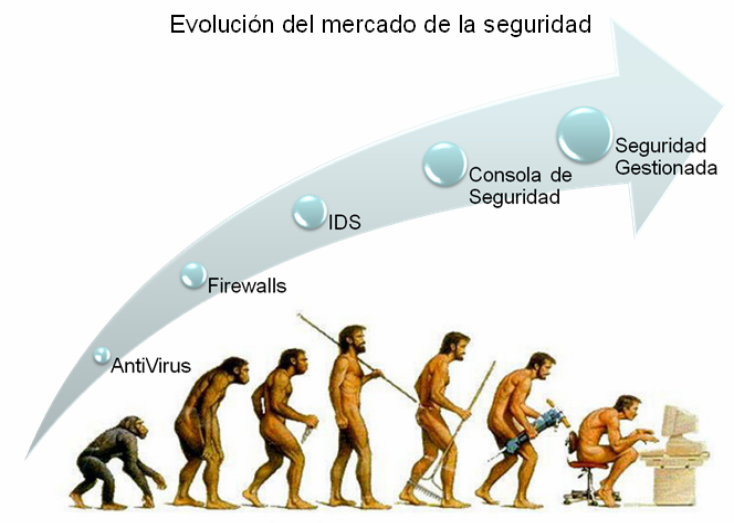

Figura 3-1. Evolución en el mercado de la seguridad[4]

[4] Imagen tomada del sitio de Open Source Security Information Management – OSSIM. http://www.ossim.net/

3.1. Políticas de Seguridad Informática

3.1.1. Definición

Una política de seguridad informática es un conjunto de reglas que definen la manera en que una organización maneja, administra, protege y asigna recursos para alcanzar el nivel de seguridad definido como objetivo[18].

Está integrada por documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos, tanto de usuarios como de administradores; describe lo que se va a proteger y de qué se está tratando de proteger.

Es una forma de comunicarse con los usuarios y el personal directivo, ya que establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son instrucciones gerenciales que trazan una dirección predeterminada o describen la forma de manejar un problema o situación; son planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras.

3.1.2. Principios fundamentales

Una Política de Seguridad Informática (PSI) debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere la disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar [19], los siguientes elementos:

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cubren el alcance de la política; estos requerimientos pueden contener estándares que aplique a un subconjunto de aplicaciones o áreas organizacionales que se encuentren dentro del alcance la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.
- Un punto muy importante dentro de las políticas es el que tienen que ir acompañadas de Sanciones, las cuales deberán también ser redactadas, revisadas, autorizadas, aplicadas y actualizadas.

Las PSI deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasará cuando algo suceda, ya que no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

3.1.3. Elementos de una Política de Seguridad Informática

El proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades en los procesos, y constancia para renovar y actualizar dicha política en función del ambiente altamente cambiante de las organizaciones y de la propia plataforma.

Los elementos que debe contemplar una política, son los siguientes:

- Declaración de intención de las políticas; alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivo de la política y descripción clara de los elementos involucrados en su definición
- Audiencia
- Clasificación de la información y de los sistemas
- Responsable de las políticas
- Fecha de inicio
- Fecha de revisión
- Publicación
- Cumplimiento
- Desviaciones
- Sanciones; definición de violaciones y de las consecuencias del no cumplimiento de la política

3.1.4. Consideraciones para establecer Políticas de Seguridad informática

Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas, donde incluye una exposición de motivos, la descripción de las personas a quienes se dirigen, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas.

Las PSI son obligatorias y pueden considerarse el equivalente de una ley propia de la organización. Debido a que su cumplimiento es obligatorio, las políticas utilizan palabras como "no se debe hacer" o "se tiene que hacer", ya que estas estructuras semánticas transmiten certeza e indispensabilidad; en caso de que un empleado desee irse por un camino que no está contemplado en la política se requiere de autorización especial.

Si bien las características de la PSI que hemos mencionado hasta el momento muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisemos algunos aspectos generales recomendados para la formulación de las mismas[20].

- Efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de la organización.
- Involucrar áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunicar a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad del área u organización.
- Desarrollar un proceso de monitoreo periódico de las directrices en el hacer de la organización que permita una actualización oportuna de las mismas.
- No dar por hecho algo que es obvio. Hacer explícito y concreto los alcances y propuestas de seguridad con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

3.1.5. Ciclo de Vida de las Política de Seguridad informática

De manera general [21], el ciclo de vida de una PSI es el siguiente:

1. Definición de la Política.
   - *Redacción*. Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo en el que participen abogados, directivos, usuarios y administradores.
   - *Edición*. Reproducir las políticas de manera formal para ser sometidas a revisión y aprobación.
   - *Aprobación*. Probablemente, la parte más difícil del proceso, puesto que es común que la gente afectada por las políticas se muestre renuente a aceptarlas. En esta etapa es fundamental contar con el apoyo de los mandos directivos.

2. Implementación de la Política.
   - *Difusión*. Dar a conocer las políticas a todo el personal de la organización mediante proyecciones de video, páginas Web, correo electrónico, cartas compromiso, memos, etcétera.

3. Verificación de su cumplimiento.
   - *Revisión*. Las políticas debe ser sometidas a revisión por un comité, que discutirá los comentarios emitidos por las personas involucradas.
   - *Aplicación*. Implementar las políticas de manera eficiente. Una política que no puede implementarse o hacerse cumplir, no tiene ninguna utilidad. Es peor tener políticas y no aplicarlas que carecer de ellas.

4. Revocación de la política.
   - *Actualización*. En el momento requerido, las políticas deberán ser revisadas y actualizadas, respondiendo a los cambios en las circunstancias; este momento "ideal" es justo después de que ocurra un incidente de seguridad.

3.1.6. Fallas frecuentes de las Políticas de Seguridad informática

Existe una serie de factores que pueden hacer que una PSI falle, entre los que se encuentran:

- Cuando no existe la PSI:
  - Argumentos de presupuesto.
  - El tamaño de la organización no lo amerita.
  - No se cuenta con personal capacitado en seguridad informática.
  - Se desconoce que son necesarias.
  - No se recibe el apoyo de los directivos, por lo cual, para fines prácticos no existe.

- Cuando existe la PSI:
  - Por debilidades naturales de las políticas:
    - La seguridad reduce la productividad y no proporciona facilidades a la operación.
    - La seguridad es un comportamiento aprendido y no es intuitivo.
    - Mientras más compleja sea una política, existe mayor probabilidad de que falle.
    - Son estáticas.

  - Por amenazas reales a la organización
    - Error humano.
    - Negligencia.
    - Falta de discreción de los participantes.

3.2. Modelos de Seguridad

Un modelo de seguridad es la presentación formal de una política de seguridad ejecutada por el sistema[5].

El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada.

Los modelos de seguridad pueden ser de dos tipos:

a) Modelo Abstracto. Se ocupa de las entidades abstractas como sujetos y objetos.
b) Modelo Concreto. Traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.

Estos modelos sirven a tres propósitos en la seguridad informática:

1. Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas.
2. Proveer una representación de una política general de seguridad formal y clara.
3. Expresar la política exigida por un sistema de cómputo específico

3.2.1. Criterios

Al asumir que la política de seguridad es realmente la apropiada, existen criterios que un modelo de seguridad debe seguir a medida que se va desarrollando para considerarse un buen modelo. Por lo tanto un modelo de seguridad debe:

- Representar de manera válida y precisa la política de seguridad. Los creadores del modelo deben explicar de manera clara cómo el modelo corresponde a la política y deben justificar la validez de las correspondencias.

- Ayudar a entender la política de seguridad a través de expresiones enfocadas y exactas y pruebas de propiedades. Un modelo ayuda a la comprensión tras aclarar conceptos y expresarlos de manera precisa, lo cual enfoca la atención sobre lo esencial.

- Soportar un análisis de seguridad. Un modelo debe soportar decisiones sobre seguridad y la verificación latente de si existe algún estado del modelo en donde una propiedad específica de seguridad no se mantiene.

- Soportar la creación y verificación del sistema. Un sistema basado en un modelo debe ser razonable para construirse y debe trabajar de manera adecuada.

- Permitir que los sistemas sean modelados en partes y después unirlas. Debe ser posible modelar sistemas complejos en partes y después unir estas partes; de esta manera cada parte será más clara y su verificación simple y correcta.

3.2.2. Modelos de Control de Acceso

Este tipo de modelos identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos sea un acceso autorizado.

También refuerzan el principio fundamental de seguridad de autorización, ya que éste protege tanto a la confidencialidad como a la integridad.

Los modelos de control de acceso son:

a) *Modelo de Matriz de Acceso*. Desarrollado a principios de los 70's para los sistemas operativos derivado de problemas de protección en sistemas multiusuarios. Este modelo relaciona los sujetos, objetos y derechos.

b) *Modelo HRU*. Modelo creado en 1976 por Harrison, Ruso y Ullman (de ahí sus nombre). Trata de mejorar el modelo de la matriz de acceso ya que éste no considera lo que un cambio en el modelo implica con respecto a la seguridad.
Este sistema de protección está constituido por un conjunto de derechos genéricos (tipos de acceso hacia un objeto como leer, escribir, borrar, modificar, ejecutar), y Un conjunto de comandos, donde cada comando cuenta con una parte condicional y una principal a fin de confrontar los derechos indicados en la matriz de acceso con la acción solicitada sobre el objeto.
Las operaciones primitivas crean y destruyen objetos y sujetos, añaden o borran derechos de la matriz de acceso.

c) *Modelo Take-Grant*. Estos sistemas representan el estado de protección mediante una gráfica dirigida, donde los derechos de un sujeto son vistos como una lista de capacidades sobre dichos objetos.

d) *Modelo Bell-LaPadula*. Este modelo formaliza la política de seguridad multinivel (clasificación de la información en los niveles no clasificado, confidencial, secreto y ultra secreto).
La información es descrita en términos de compartimientos los cuales representan el asunto del sujeto El nivel de seguridad o clase de acceso de un documento es la combinación de su nivel y conjunto de compartimientos. Cualquier personal autorizada recibe un permiso para un cierto nivel, de esta manera tanto las personas como la información tienen niveles de seguridad o clases de acceso.

3.2.3. Modelos de Flujo de Información

Considerando que la información actualmente se ha convertido en uno de los activos más importantes para las organizaciones, ésta debe ser protegida.

A continuación se presentan los diversos modelos de protección para el flujo de información.

a) *Teoría de la Información*. Esta teoría define la información en términos de incertidumbre; al proporcionar información se elimina la incertidumbre.

b) *Modelo enrejado del flujo de información*. Una política de flujo de información define las clases de información que un sistema puede tener y cómo la información puede fluir entre esas clases.
Un modelo de flujo de información puede expresar la política de multinivel en términos del flujo de información más que en el control de acceso; la política del flujo está definida por un enrejado. Un enrejado es una estructura matemática que representa el significado de los niveles de seguridad.

3.2.4. Modelos de Integridad

Estos modelos están enfocados a la protección de la información de manera que ésta no sufra modificaciones que no hayan sido autorizadas.

a) *Modelo Biba*. Modelo creado por K.J. Biba en 1977.
El modelo de integridad supone un enrejado de niveles de integridad con una relación ordenada menor o igual. Los objetos son asignados a clases de integridad de acuerdo con el daño que sufrirían si fueran modificados de manera inapropiada. Los usuarios son asignados a clases de integridad basados en su veracidad.

b) *Modelo de Clark-Wilson* fue desarrollado por David Clark y David Wilson entre 1987 y 1989. aunque no es un modelo altamente formal, es un armazón para describir los requerimientos de la integridad.
Clark y Wilson demostraron que para la mayoría del cómputo relacionado con las operaciones de negocios y el control de los recursos, la integridad es más importante que la confidencialidad.

Ellos argumentaban que las políticas de integridad demandan modelos diferentes a los modelos de confidencialidad y diferentes mecanismos ya que se enfocan en dos controles que son centrales en el mundo comercial: las transacciones bien formadas y la separación de la obligación.

3.3. Identificación y establecimiento de políticas de seguridad

Para que una PSI logre su implementación dentro de cualquier organización, ésta debe integrarse a las estrategias del negocio, a su misión y visión a fin de que los niveles gerenciales o directivos reconozcan su importancia e implicaciones en las actividades de la organización.

En términos gerenciales, las PSI se utilizan para definir un nivel mínimo de protección, llamado también *línea de base*; por ello, las políticas representan una manera definitiva mediante la cual la dirección puede demostrar la importancia de la Seguridad Informática, además de representar una forma relativamente barata y directa de definir el comportamiento correcto que los trabajadores tienen la obligación de acatar.

El entender a la organización, sus elementos culturales y comportamiento del personal ayudan en el reconocimiento de las pautas de seguridad necesarias y suficientes que aseguren la confiabilidad en las operaciones y funcionalidad de cualquier organización.

Algunas reglas que deben considerarse al establecer una política de seguridad son las siguientes:

- Toda política de seguridad debe cubrir todos los aspectos relacionados con el sistema.
- Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.
- Debe tomar en cuenta los distintos componentes del sistema –hardware, software, entorno físico y usuarios- así como la interacción entre los mismos.
- Debe tomar en cuenta el entorno del sistema, esto es, el tipo de compañía o entidad: comercial, bancaria, educativa, de investigación, etcétera.
- La política de seguridad debe adecuarse a las necesidades y recursos, el valor que se le da a los recursos y a la información, así como al uso que se hace del sistema en todos los departamentos.
- Deben evaluarse los riesgos, el valor del sistema protegido y el costo de ser atacado; las medidas de seguridad tomadas deben ser proporcionales a estos valores.
- Debe adoptar el modelo "Todo lo que no esté específicamente prohibido está permitido", o mejor aún "Todo está prohibido excepto lo que está específicamente permitido".

Asociado a las políticas de seguridad informática se encuentran los planes de contingencia, mismos que permiten a la organización continuar operando de manera correcta en caso de presentarse algún inconveniente en la infraestructura de comunicaciones.

3.4. Plan de Continuidad del Negocio

Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de los involucrados en la administración de recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

El principal objetivo es reaccionar ante la interrupción de alguna actividad, sustantiva o no, de la organización y proteger los procesos críticos ante fallas y desastres mediante la combinación de controles preventivos y de recuperación.

De acuerdo con MetroRed[5], un plan de continuidad del negocio debe contemplar los aspectos indicados en la Figura 3-2. Cada elemento se describe en la Tabla 3-1.

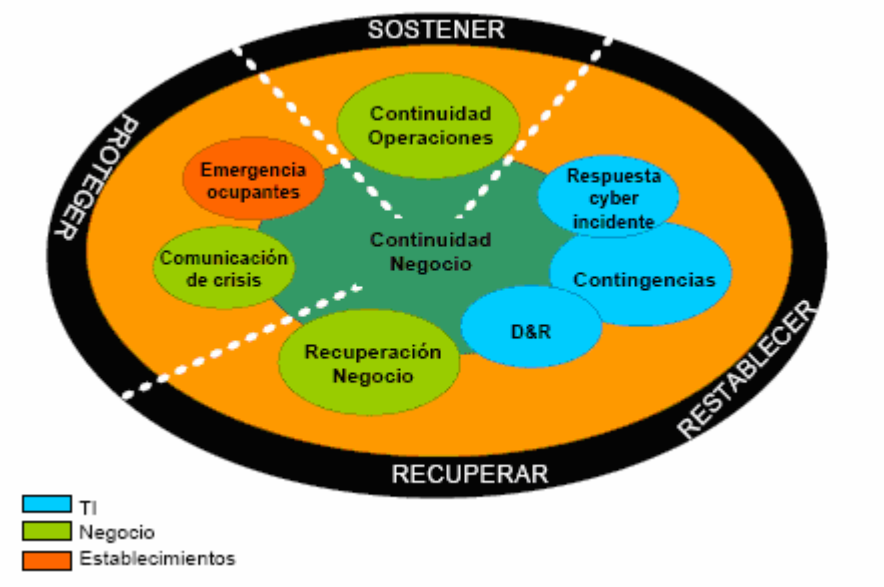

Figura 3-2. Plan de continuidad del Negocio

[5] México Red de Telecomunicaciones, S. de R.L. de C.V. (Metrored), es una empresa de telecomunicaciones.

Plan	Objetivo
Plan de Continuidad del Negocio (BCP)	Proporciona procedimientos para sostener las operaciones críticas de un negocio recuperándose de una interrupción significativa
Plan de Recuperación de Negocio (BRP)	Proporciona procedimientos para restablecer las operaciones inmediatamente después de un desastre (incluye procesos de negocio; sólo incluye las TI como soporte de los procesos de negocio)
Plan de Continuidad de Operaciones (COOP)	Proporciona procedimientos y capacidades para sostener las funciones críticas y estratégicas de una organización en una localización alternativas hasta 30 días (incluye el conjunto de las misiones más críticas; no se centra en las TI)
Plan de Contingencias IT	Proporciona procedimientos y capacidades para restaurar aplicaciones críticas o sistemas de soporte general (se centra en las interrupciones de los sistemas TI, no en los procesos de negocio)
Plan de Comunicaciones de Crisis	Proporciona procedimientos para distribuir informes y regular las comunicaciones con el personal y con el público (no está basado en las TI)
Plan de Respuesta ante cyber-incidentes	Proporciona estrategias para detectar, responder y limitar las consecuencias de un cyber-incidente malicioso (se centra en las respuestas a incidentes que afectan a sistemas y/o redes)
Disaster&Recovery Plan (DRP)	Proporciona procedimientos detallados e instrucciones técnicas para facilitar la recuperación de las capacidades en un centro alternativo (basado en las TI)
Plan de Emergencia de Ocupantes (OEP)	Proporciona procedimientos coordinados para minimizar los daños acontecidos en caso de determinados sucesos físicos (se centra en el personal y en recursos físicos concretos, no en los procesos de negocio o en los sistemas TI)

Tabla 3-1. Planes de contingencia

3.5. Procedimientos y planes de contingencia

Mientras las políticas indican el "qué hacer", los procedimientos indican el "cómo hacer". Los procedimientos son los que nos permiten llevar a cabo las políticas establecidas.

Los planes y procedimientos de contingencia están encaminados a conseguir la restauración progresiva y ágil de los servicios asociados a una organización afectados por una interrupción, total o parcial, de su capacidad operativa.

De acuerdo con Luis Villablanca V., jefe del área de consultoría de SONDA, S.A.[6], cualquier organización debe realizarse las siguientes preguntas para saber su nivel de seguridad con respecto a la continuidad del negocio:

[6] Empresa chilena proveedora de soluciones TI.

- ¿Cuáles son los procesos críticos para la continuidad de mi negocio?
- ¿Qué nivel de dependencia tienen mis procesos críticos con relación a las tecnologías de información que los apoyan?
- ¿Cuáles son las fallas que pueden ocurrir que ponen en riesgo la continuidad de operación de mis procesos críticos?
- ¿Cuál es el tiempo de reposición de los servicios informáticos dada mi infraestructura informática actual?
- ¿Cuál es la probabilidad de ocurrencia de estas fallas?
- En caso de ocurrir una falla ¿cuál es el impacto que ésta genera sobre mi negocio?

Estar preparado para estas contingencias implica realizar inversiones orientadas a dar alta disponibilidad al equipamiento y comunicaciones críticas, implementar sitios alternativos preparados para prestar los servicios ante una situación anómala en el sitio principal, definir procedimientos de contingencia, capacitar al personal en como actuar frente a ellas y ejecutar pruebas periódicas de las soluciones de contingencia.

Frente a esta necesidad surge la pregunta, ¿Cuánto debo invertir en mi proyecto de Contingencia Informática? Claramente el monto de la inversión debe ser menor que el riesgo potencial que se está corriendo frente a una contingencia.

El impacto sobre el negocio de los desastres informáticos no sólo corresponde a hechos cuantificables económicamente tales como pérdida de ventas, pago de multas, costo financiero de postergación de ingresos, etc., sino que también deben ser considerados impactos cualitativos que muchas veces son de mayor relevancia para el negocio, por ejemplo los siguientes:

1. Deterioro de la imagen de la empresa frente a los clientes, accionistas, empleados, entidades regulatorias y proveedores.
2. Aumento de barreras para conseguir financiamiento en el futuro.
3. Aumento de barreras para el ingreso a nuevos negocios en el futuro.

Solamente conociendo el impacto de los desastres informáticos sobre el negocio es posible tomar la decisión de cuánto invertir en una solución de contingencia, y con ello poder elegir entre las múltiples alternativas técnicas que presenta el mercado para mantener la continuidad del negocio frente a situaciones complejas e imprevistas.

Estas alternativas deben considerar diversos momentos para alguna eventualidad: antes, durante y después, ya que para cada momento se tendrá un costo distinto con sus subsecuentes pérdidas.

3.5.1. Procedimientos preventivos

Los procedimientos preventivos son todas aquellas actividades de planeación, preparación, entrenamiento y ejecución de acciones asociadas al resguardo de la información cuyo objetivo es el aseguramiento de un proceso de recuperación con el menor costo posible para la organización.

Estas actividades generales las podemos dividir en

- ***Establecimiento del Plan de Acción***
  Contempla los procedimientos relativos a:
  a) Sistemas de Información
  Sistemas de Información utilizados en la operación diaria de la organización. Se debe identificar toda información, automatizada o no, necesaria para su operación.
  Una vez identificados los sistemas, se deberá priorizar su importancia para que la organización pueda recuperar su operatividad en caso de desastre.

  b) Equipos de Cómputo
  - Inventario actualizado de los equipos de manejo de información, indicando su ubicación y nivel de uso institucional.
  - Pólizas de seguros comerciales, como parte de la protección de los activos de la organización. En el caso del equipo de cómputo, se debe considerar una cláusula que indique que el equipo siniestrado será sustituido por orto de mayor potencia debido a las actualizaciones tecnológicas, siempre y cuando se encuentre dentro de los montos asegurados.
  - Señalización o etiquetado de los equipos de acuerdo a la importancia de su contenido a fin de priorizarlos en caso de evaluación.
  - Tener actualizada una relación de PC's requeridas como mínimo para cada sistema de la organización, las funciones que realizará y la frecuencia de uso a fin de satisfacer las necesidades de operación.

  c) Obtención y almacenamiento de los respaldos de información (Backup)
  Establecer procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas de información, para lo cual se debe contar con:
  - Respaldo del Sistema Operativo. Si se tiene más de un SO o versión, se deberá tener una copia para cada uno de ellos.
  - Respaldo de paquetes y lenguajes de programación básicos mediante los cuales se realizan los desarrollo de la organización
  - Respaldo del software aplicativo (programas fuente, programas objeto y cualquier otro software o procedimiento que trabaje con la información a fin de producir los resultados con los cuales trabaje el usuario final). De igual manera, se deben considerar las copias de los listados fuente en caso de problemas.
  - Respaldo de los datos (Base de datos, estructura, índices, tablas de validación y password) bitácoras y todo archivo de datos asociado a las operaciones de la organización.

  d) Políticas (Normas y Procedimientos de respaldos)
  Se debe establecer los procedimientos, normas y determinación de responsabilidades en la obtención de respaldos mencionados en el punto c), lo cual debe incluir:
  - Periodicidad de cada tipo de respaldo
  - Respaldo de información de movimientos realizados durante los periodos en que no se realizan respaldos (respaldos incrementales)
  - Uso obligatorio de un formulario estándar para el registro y control de respaldos.

- Correspondencia entre la relación de sistemas e información necesarios para el buen funcionamiento de la organización, y los respaldos efectuados.
- Almacenamiento de los respaldos en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de respaldos en forma periódica a fin de evitar su pérdida por el deterioro del medio magnético utilizado
- Almacenamiento de respaldos en sitios físico distintos a donde reside la información a fin de mantener resguardada la información en caso de desastre en el área.
- Pruebas periódicas de los respaldos (restore) a fin de verificar su funcionalidad, a través del sistema, comparando contra resultados anteriores confiables.

La Figura 3-3 muestra los distintos tipos de respaldo que pueden realizarse considerando el tamaño de las organizaciones.

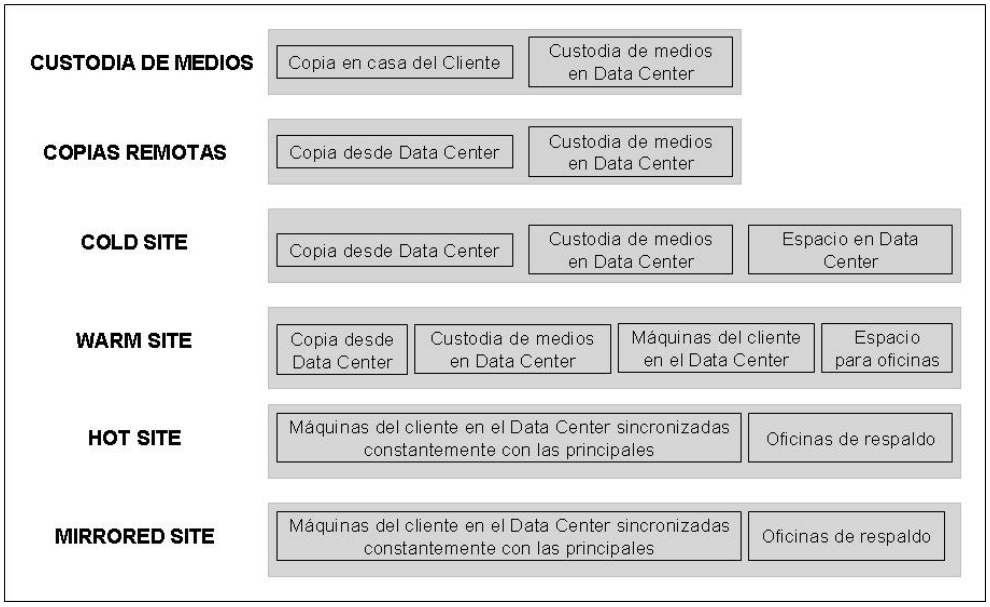

Figura 3-3. Opciones de Respaldo

- ***Formación de Equipos Operativos***

En cada un unidad operativa de la organización, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de dicha unidad.

Entre sus responsabilidades podemos listar:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc. para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.

- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, módems, y otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el sitio alternativo.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el sitio alternativo.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas simulacros de desastres.

- ***Formación de Equipos de Evaluación***
  Esta función debe ser realizada de preferencia por personal de auditoría; de no ser posible, la realizará el personal del área de informática debiendo establecerse claramente sus funciones, responsabilidades y objetivos, entre los que podemos mencionar:

  - Revisar que las Normas y Procedimientos con respecto a los respaldos, seguridad de equipos y de información se cumpla.
  - Supervisar la realización periódica de los respaldos, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
  - Revisar la correlación entre la relación de Sistemas e Información necesarios para el buen funcionamiento de la organización y los respaldos realizados.
  - Informar de los cumplimientos e incumplimientos de las Normas para las acciones correctivas correspondientes.

3.5.2. Procedimientos correctivos

Los procedimientos correctivos deben aplicarse una vez que ha sucedido un ataque o contingencia. Para ello se debe llevar a cabo el procedimiento previamente establecido.

3.5.3. Plan de Recuperación de Desastres

Un Plan de Recuperación de Desastres, o Plan de Contingencia[W11], es el conjunto de procedimientos alternativos a la operación normal de una organización, cuyo objetivo es definir las pautas necesarias para una adecuada recuperación de la información, en caso de ser necesario, y permitir su funcionamiento cuando alguna de sus divisiones deje de funcionar debido a algún incidente ya sea interno o ajeno a la organización mediante una metodología definida para recuperar el procesamiento de recursos críticos.

Las causas pueden ser variadas y van desde un problema informático, un fallo en el correcto flujo de la información o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones.

El hecho de preparar un plan de contingencia no implica un reconocimiento de la ineficiencia en la administración de la organización, por el contrario, supone un importante avance en cuanto a prevención y superación de situaciones adversas que pueden provocar importantes pérdidas, no solo a nivel material, sino aquellas derivadas de la paralización de la operación durante un período más o menos largo.

Su elaboración la podemos dividir en las siguientes etapas:

1. Evaluación.
2. Planificación.
3. Pruebas de viabilidad.
4. Ejecución.
5. Recuperación.

Las tres primeras hacen referencia al componente preventivo y las últimas a la ejecución del plan una vez ocurrido el siniestro.

Considerando que el objetivo principal de un plan de contingencia es la continuidad de las operaciones de la organización, no sólo de sus sistemas de información, un plan de contingencia deberá abarcar los siguientes aspectos:

1.- Plan de Reducción de Riesgos (Plan de Seguridad).
2.- Plan de Recuperación de Desastres.
- 2.1.- Actividades Previas al Desastre.
  - 2.1.1.- Establecimiento del Plan de Acción.
    - a) Sistemas de Información
    - b) Equipos de Cómputo
    - c) Obtención y almacenamiento de los respaldos de información (Backups)
    - d) Políticas (Normas y procedimientos de backups)
  - 2.1.2.- Formación de Equipos Operativos.
  - 2.1.3.- Formación de Equipos de Evaluación (auditoria de cumplimiento de procedimientos de Seguridad).
- 2.2.- Actividades durante el Desastre.
  - 2.2.1.- Plan de Emergencias.
  - 2.2.2.- Formación de Equipos.
  - 2.2.3.- Entrenamiento.
- 2.3.- Actividades después del Desastre.
  - 2.3.1.- Evaluación de Daños.
  - 2.3.2.- Priorización de Actividades del Plan de Acción señaladas en 2.1.1
  - 2.3.3.- Ejecución de Actividades
  - 2.3.4.- Evaluación de Resultados.
  - 2.3.5.- Retroalimentación del Plan de Acción.

Debido a la alta dependencia que actualmente se tiene de los sistemas informáticos, para la continuidad del negocio debemos contar con un Plan de Continuidad Operativa del Negocio

(Business Continuity Planning) y con un Plan de Contingencia Tecnológico (Disaster Recovery Plan), con los aspectos indicados en la Tabla 3-2.

Plan de Continuidad Operativa del Negocio **(Business Continuity Planning)**	**Plan de Recuperación al Desastre** **(Disaster Recovery Plan)**
Este plan permite recuperar los servicios del negocio, en el menor tiempo posible, de acuerdo a las definiciones de procesos críticos, su impacto y recursos destinados para la organización. Este Plan de Continuidad de Negocio incluye, al menos, los siguientes documentos: • Definición de procesos críticos • Definición de escenarios de fallas • Análisis de impacto • Matriz de escenarios de fallas vs procesos críticos • Definición de estrategias de recuperación • Definición de usuarios críticos • Escalamiento de eventos de contingencia • Comunicados en contingencia • Definición de proveedores críticos • Procedimientos de contingencias alternativos • Plan de pruebas • Capacitación y difusión	Este plan es un subconjunto y complemento necesario para el Plan de Continuidad Operativa del Negocio. Está enfocado a resolver las contingencias tecnológicas (escenarios de falla) que impidan entregar los servicios informáticos necesarios que requieren los procesos críticos del Negocio. Debe incluir • Definición de procesos críticos • Definición de escenarios de fallas • Definición de servicios críticos • Definición de site secundario o site alternativo • Definición de modalidad de operación de sites: o Activo-Activo o Activo-Pasivo o Pasivo-activo • Procedimientos de contingencias alternativos: o Condiciones previas (para poder ejecutar el procedimiento alternativo) o Forma de activación, responsables, encargados o Transición a la normalidad (vuelta atrás) • Plan de pruebas

Tabla 3-2. Plan de Continuidad del Negocio y Plan de Recuperación al Desastre

Para la realización del BCP se contemplan las siguientes fases:

Fase I. Análisis y diseño de la estrategia de respaldo. Estudio de la problemática, necesidades de recursos, alternativas de respaldo y su costo/beneficio.

Fase II. Implantación del plan de contingencias. Organización de los equipos de emergencia y desarrollo de los procedimientos y planes de actuación para las distintas áreas y equipos.

Fase III. Prueba del plan de contingencias. Definición de las pruebas, realización de las pruebas y refinamiento de las mismas.

Fase IV. Mantenimiento del plan de contingencias. Definición de los procedimientos de mantenimiento.

3.6. Sistemas y mecanismos de Protección

Toda organización debe contar con sistemas y mecanismos de protección que garanticen la continuidad del negocio a fin de evitar el mayor número posible de vulnerabilidades que permitan un ataque.

Estos mecanismos de protección deberán poder ser aplicados antes, durante y después de cualquier eventualidad en la infraestructura y comunicaciones de la organización, por lo que un sistema de protección debe considerar los siguientes aspectos indicados en la Figura 3-4.

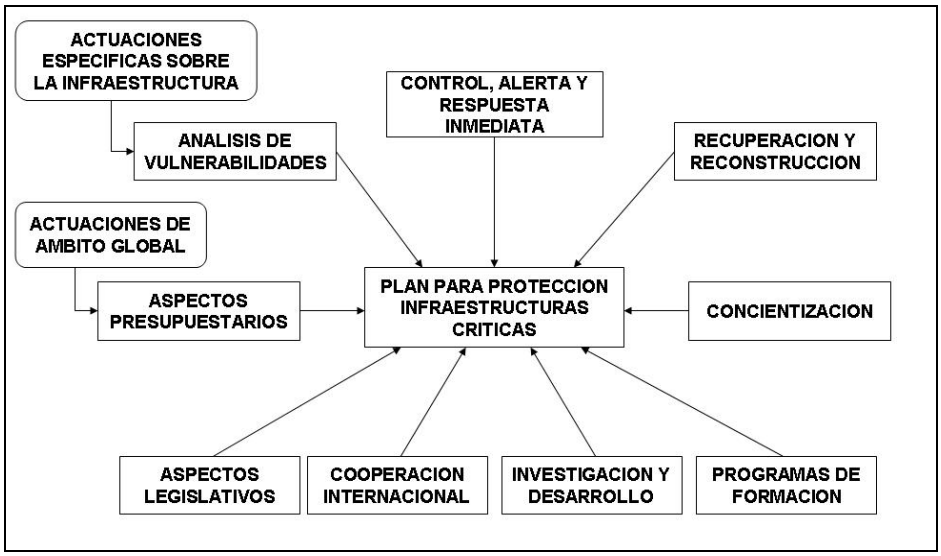

Figura 3-4. Plan de Protección para Infraestructuras Críticas

- *Análisis y vulnerabilidad*. Para cada sector de la organización y de manera periódica para conocer las vulnerabilidades existentes y la infraestructura mínima esencial de cada área. También deben elaborarse planes para la disminución de dicha vulnerabilidad.

- *Control y alerta*. Mediante la implantación de centros que permitan el control de las redes y la alerta temprana en caso de ataques a los sistemas de información.

- *Respuesta y reconstrucción*. Previsiones para las respuestas a los ataques, reconstrucción de las infraestructuras y planes de contingencia.

- *Programas de formación y concienciación*. El objeto es hacer comprender a los operadores y usuarios de las infraestructuras críticas la importancia que tiene la implantación de las medidas de seguridad.

- *Programas de Investigación y Desarrollo*. Que tengan como objetivo la creación de tecnologías y herramientas para la seguridad y la protección de las infraestructuras críticas.

- *Aspectos legislativos y presupuestarios* para crear el marco adecuado que permita la implantación y desarrollo de las medidas de protección.

Como se puede observar, los tres primeros elementos actuarían específicamente sobre las infraestructuras críticas objeto de protección mientras que el resto son actuaciones que tienen un carácter global en toda la organización.

En realidad, estas tres acciones se realizarán en el tiempo antes, durante y después de un ataque hacia los sistemas de información. Es decir, los análisis de vulnerabilidad son preventivos y previos a un ataque. Los mecanismos de control y alerta son la respuesta a un posible ataque y la recuperación y reconstrucción son acciones posteriores a un ataque cuando éste haya tenido un cierto éxito.

3.6.1. Seguridad física

La seguridad física se refiere al aseguramiento de las instalaciones físicas de la organización, tal como la ubicación de los centros de procesos, protecciones físicas, medidas contra incendios, inundaciones, terremotos y cualquier siniestro que pueda afectar dichas instalaciones.

Entre los requisitos de seguridad podemos listar:

- Control físico de entrada, tanto para personal como para visitantes
- Control de acceso y salida de paquetes
- Suministro eléctrico
- Seguridad del Cableado
- Temperatura del site
- Áreas de tráfico
- Implementación de cámaras de seguridad
- Asignación de responsables por área de operación

3.6.2. Seguridad lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo se permita el acceso a aquellas personas autorizadas para hacerlo, es por ello que debe ser implementada en todos los procesos asociados al manejo de la información, así como a los canales que se utilizan para su transmisión.

Esta seguridad debe ser implementada mediante controles de accesos a la información exigiendo la identificación y autenticación del usuario, o mediante el cifrado de de la información en dispositivos físicos, o durante su transmisión en línea.

Ejemplos de seguridad lógica son los siguientes:

- Segmentación de la red
- Detección y protección contra intrusos
- Instalación y configuración de firewalls y proxies
- Autenticación y verificación de identidad de usuarios
- Criptografía y criptoanálisis

3.6.3. Seguridad en el modelo TCPI/IP

La seguridad de la red no debe verse sólo como un problema en una capa específica del protocolo TCP/IP, sino que debe verse como un conjunto de procedimientos a implementar en cada una de ellas.

3.6.3.1. Capa física

En esta capa, debido a la arquitectura del protocolo, se utiliza el broadcast lo que implica que todos los equipos conectados a la red "escuchan" todo el flujo de información que viaja a través de la red, lo cual es un peligro potencial cuando existe alguna usurpación de dirección MAC.

3.6.3.2. Acceso a la Red

El modelo de seguridad de red se enfoca en controlar el acceso a la red, y no en asegurar los hosts en sí mismos. Este modelo está diseñado para tratar los problemas identificados en el ambiente de seguridad de hosts, aplicando los mecanismos de protección en un lugar en común por el cual circula todo el tráfico desde y hacia los hosts: los puntos de acceso a la red.

Un enfoque de seguridad de acceso a la red involucra la construcción de firewalls para proteger redes confiables de redes no confiables, utilizando sólidas técnicas de autenticación, y usando encriptación para proteger la confidencialidad e integridad de los datos a medida que atraviesan la red.

La ventaja sobre el modelo de seguridad de hosts es una considerable reducción del costo para proveer la misma o mejor protección, ya que sólo se necesita proteger unos pocos puntos de acceso (en muchos casos, sólo uno) lo que permite concentrar todos los esfuerzos en una solución perimetral. Este modelo es escalable en la medida de que la solución perimetral pueda soportar los cambios sin afectar su desempeño.

Una desventaja de este modelo es que es muy dependiente de algunos pocos puntos de acceso por lo que pueden producirse reducciones en el desempeño del tráfico de entrada y salida de la red; por otro lado, la protección lograda no es flexible y posee un bajo grado de granularidad, es decir, no es posible especializar la protección necesaria para cada host y sistema final de la red privada.
Para poder mantener la seguridad en la red, ésta se debe mantener actualizada en cuanto al descubrimiento de vulnerabilidades y poder así aplicar el respectivo parche que las resuelve, actualizando las versiones en todos los equipos de la red.

Otra forma de proteger la red es a través de la revisión de los log de transacciones de aplicaciones y dispositivos de red.

a) Segmentación de la red

La segmentación de la red controla el flujo del tráfico entre los hosts de los distintos segmentos de una red. Una red segmentada, si se ha diseñado correctamente, mejora el rendimiento y la seguridad, ya que garantiza que sólo el tráfico adecuado se reenvía entre los segmentos de la red. El cambio de concentradores a conmutadores puede reducir la capacidad de un pirata informático para rastrear contraseñas y otro tráfico confidencial de la red, pero los conmutadores no eliminan esa posibilidad. Un sistema en peligro conectado a un conmutador aún se puede utilizar para recopilar información de otros sistemas. Por este motivo, debe considerar los conmutadores como una respuesta apropiada para las colisiones y el rendimiento de la red, y no su seguridad.

El filtrado de puertos y paquetes, en combinación con servidores de seguridad personales, también puede contribuir a proteger los sistemas antiguos de intrusiones y amenazas. No obstante, en algunas situaciones no resulta práctico instalar y administrar software de servidor de seguridad en los equipos de los usuarios debido a la carga administrativa que suponen. A menos que se instale un software de servidor de seguridad que se pueda administrar y configurar de forma remota mediante un servidor y una base de datos centrales, un administrador tendrá que acceder a cada equipo numerosas veces después de la implementación para modificar la configuración con el fin de atender las necesidades de cada usuario. También se incrementa la probabilidad de que se tengan que realizar tareas administrativas adicionales por cada nueva aplicación que se implemente en respuesta a las vulnerabilidades adicionales y puntos de error que la aplicación pueda introducir.

Algunas organizaciones no disponen del personal necesario para administrar un potencial de cientos de servidores personales. En estas situaciones, las organizaciones pueden optar por la segmentación de la red como un mecanismo de seguridad alternativo o adicional con el fin de proporcionar protección adicional a la red. La segmentación de la red implica poner en cuarentena a determinados servidores en una red perimetral; de igual manera, implica dividir la red en segmentos discretos para proporcionar niveles adicionales de seguridad a los sistemas que se encuentran en cada segmento. La segmentación también puede ofrecer una flexibilidad considerable para modelar el tráfico, supervisar y filtrar los puertos, así como otras tareas de administración de red, ya que cada segmento puede disponer, potencialmente, de su propia configuración discreta que se adapte a las necesidades de los usuarios del grupo a la vez que se adecua a las necesidades de seguridad de la red.

La segmentación de la red soluciona dos amenazas posibles: las que proceden del exterior de la red y las que surgen desde el interior de la misma; permite estructurar la red en zonas de seguridad discretas con la capacidad de una administración del tráfico única y basada en reglas de cada segmento. La red se puede segmentar de varias formas. Por ejemplo, puede optar por implementar un servidor de seguridad basado en hardware en cada segmento y segmentar físicamente la red; o bien puede implementar un único servidor de seguridad centralizado con capacidad de LAN/segmentación virtual que sirva para proteger grupos individuales.

La solución final dependerá de la topología de la red y las necesidades de seguridad de cada grupo. Como mínimo, se debe aislar los segmentos que suponen un mayor riesgo, como las redes inalámbricas, del resto de la red e imponer reglas estrictas para impedir el tráfico no autorizado hacia estos segmentos o desde ellos.

b) Filtrado de paquetes

Un firewall de este tipo acepta o rechaza el tráfico de la red dependiendo de la información de las cabeceras de los paquetes de los protocolos TCP e IP. Este tipo de solución es más económica pero aporta un grado menor de protección que otros tipos. Tiene la ventaja de afectar muy poco al rendimiento de la red.

Puntos débiles del filtrado de paquetes

1. Debido a que los filtros de paquetes no analizan los datos propios de los niveles superiores del modelo OSI, no se puede impedir ataques que utilizan las vulnerabilidades de las aplicaciones y otras funciones.
2. Debido a la escasa información que dispone el firewall, su funcionalidad de archivo de eventos queda muy limitada. Esta información se limita a las direcciones de origen, de destino y tipo de paquetes.
3. La mayor parte de los filtros de paquetes no permiten esquemas de identificación de usuario. Esta limitación se asocia a la escasez de funciones a nivel superior del firewall.
4. Este tipo de firewall son vulnerables a ataques que utilizan las particularidades de TCP/IP. Muchos firewall de filtros de paquetes no pueden detectar paquetes en los que la información de direcciones a nivel de red del modelo OSI ha sido modificada. Este tipo de ataques son utilizados por intrusos para soslayar los controles de seguridad existentes en los firewalls.
5. Debido al escaso número de variables utilizadas para las decisiones de control, estos firewall están sometidos a las debilidades causadas por configuraciones incorrectas. Por ejemplo, frecuentemente se da el caso de configurar un firewall de este tipo que permite tipos de paquetes, con orígenes y destinos que deberían ser bloqueados basándose en la política de seguridad establecida.

c) Firewalls y proxies

Un firewall es un sistema o grupo de sistemas que refuerzan la política de control de acceso entre dos redes, permitiendo el aislar la red privada de lo que es Internet, por lo que en su configuración se debe permitir el acceso a servicios específicos y prohibir el resto.

Los firewalls presentan una sencillez en su configuración así como la aplicación de arquitecturas multicapa para cada tipo de segmento de la red: interno, externo (típicamente Internet), y zonas intermedias conocidas como DMZ (*DeMilitarized Zones*).

En toda implementación de un firewall se debe balancear la seguridad y la accesibilidad, implementando restricciones en base a las necesidades de cada organización. También debe hacerse énfasis en que la comunicación con la consola de gestión del firewall debe viajar de forma encriptada.

Ventajas:

- Sólo dejan abiertos los puertos 80 y 443
- Detienen algunos ataques DoS

Desventajas:

- No entiende el significado de http
- Dejan pasar el 100% de los ataques web

Existen tres tipos de firewall:

- Filtrado de paquetes (*stateless*)
  Fue la primera tecnología empleada en el control de acceso de las redes, y suele ser implementada mediante listas de control de aceso, que especifican el tráfico que puede pasar a través del filtro de los valores existentes en las cabeceras TCP, UDP e IP: direcciones IP y puertos UDP y TCP.

  Suelen caracterizarse por una gestión muy compleja debido al elevado número de reglas que debe especificarse, ya que la orientación de su diseño se basa en el análisis de cada paquete individual que pasa por la red.

  No se adaptan a protocolos dinámicos como puede ser FTP, en los que los puertos por los que se realizarán ciertas comunicaciones se determinan en el transcurso de la conexión; no están predefinidos inicialmente.

  Por otro lado, no pueden manejar de forma seguro los protocolos basados en UDP, ya que no se dispone en el momento de su configuración de los puertos UDP aleatorios elegidos por los clientes internos de la red, por lo que para habilitar la comunicación es necesario abrir todos los puertos mayores al 1023.

- Proxy de aplicación
  Un tipo particular de este tipo de firewall basados en proxies, y el más sencillo, es el de traductores de protocolos genéricos, como SOCKs. Estos se encargan de reenviar las peticiones de red (mediante llamadas *sockets*) haciendo intermediarios, pero sin aplicar ningún filtro a los datos.

  Por otro lado, los proxies de aplicación específicos disponen de información propia de la aplicación, por lo que son capaces de aplicar restricciones muy particulares, como por ejemplo en el caso del protocolo http no permite la obtención de applets Java, o en el caso de FTP, permite enviar información (put) pero no recibirla (get).

  Debido a este conocimiento detallado de la aplicación se trata de sistemas más seguros, siempre que se disponga de un filtro específico asociado a la aplicación o protocolo que se desea filtrar. En caso contrario suponen una desventaja, ya que en el caso de nuevas aplicaciones no se dispondrá de dicho filtro, por lo que se deberá aplicar un proxy genérico.

  Si se realiza un análisis a muy bajo nivel se contará con una auditoría muy detallada, pero su costo será un menor rendimiento debido a la complejidad de operaciones.

- Filtros con estado (*stateful filtres*)
  Los filtros con estado trabajan, por diseño, con las conexiones o sesiones, no con paquetes individuales, y son inteligentes desde el punto de vista que controlan cada paquete asociado a cada conexión que pasa a través de ellos, siendo conscientes de los pasos posibles a realizar por la aplicación o el protocolo.

  La configuración es sencilla, ya que debido al conocimiento intrínseco al firewall, con especificar el tráfico deseado, se configurarán automáticamente los caminos necesarios para el tráfico de retorno. Por esto, es capaz de trabajar con protozoos dinámicos como FTP.

  La seguridad que añaden y el rendimiento obtenido es muy positivo. Como desventaja se puede señalar la dificultad para analizar los contenidos de las aplicaciones, centrándose más en los protocolos, como TCP y UDP.

d) Detección y prevención de intrusos (IDS/IPS)

Los sistemas de detección de intrusos (IDS, *Intrusion Detection System*) proporcionan un mayor control sobre la seguridad ya que pretenden contemplar dentro de sus comprobaciones todas y cada una de las vulnerabilidades que se van descubriendo a nivel de TCP/IP y de los servicios de red.

Los IDS suelen conformarse mediante un sistema de gestión centralizado y agentes o monitores remotos que se encargan de analizar el tráfico en los puntos remotos de la red en los que están ubicados. La comunicación entre los agentes y el gestor no se realiza a través del protocolo SNMP como ocurre en los entornos de gestión de red, sino que la comunicación se establece de forma más segura, con métodos de autentificación y codificación.

Ciertos IDS permiten la introducción de nuevos patrones (*signatures*), de forma que es posible empliar la base de datos de vulnerabilidades en el momento en que aparecen, y no tener que esperar a que el fabricante distribuya la actualización.

En conjunto con el IDS se puede utilizar un sistema de prevención de intrusos (IPS, *Intrusion Prevention System*), que es un dispositivo que vigila la red y/o actividades de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o impedir dichas actividades. Como los IPS originalmente fueron una extensión de los IDS, ambos siguen siendo relacionados al considerarse tecnologías coplementarias.

Como ventaja considerable es que un IPS puede hacer que el control de acceso de lleve a cabo basado en una solicitud de contenido, en lugar de direcciones IP o los puertos tradicionales que venían haciendo los firewalls.

Ventajas:

- Detecta los ataques antes de que lleguen al servidor

Desventajas:

- No detecta ataques lógicos
- Problemas de escalamiento

e) Autenticación y autorización de servicios

La autenticación generalmente se da a través de esquemas de contraseñas, las cuales si no cuentan con una política robusta de generación y mantenimiento se vuelven fácilmente vulnerables.

Un esquema de autenticación seguro es *kerberos*, el cual se utiliza para autenticar el uso de servicios como NFS. Kerberos se basa en un esquema de boletos entregados para la autenticación y de dos llaves secretas, una dada por kerberos y otra conocida por los usuarios para entrar al sistema.

Un esquema básico de protección se basa en una matriz de acceso, en la cual se listan los recursos y las actividades que se pueden realizar sobre él; sin embargo estas matrices no son tan eficientes ya que dependen de la cantidad de recursos, de usuarios y frecuencia de accesos.

Un mejor esquema son las listas de control de acceso en las cuales se puede especificar el acceso a cada recurso de una forma más eficiente.

Un esquema de protección mejor aún es el acceso a través de roles, mediante el cual se controla el acceso dependiendo del nivel de seguridad de la información.

f) Criptografía y criptoanálisis

La palabra criptología proviene de las palabras griegas *krypto* y *logos*, que significa estudio de lo oculto; es la ciencia que combina la criptografía y el criptoanálisis.

Una rama de la criptología es la *criptografía*, que se ocupa del cifrado de mensajes basada en la aritmética. Su forma de operación es que el emisor emite un mensaje en texto claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado en forma de bits ya que los equipos informáticos usan el sistema binario. Este texto cifrado llega al descifrador a través del canal de comunicación establecido, y éste a su vez convierte el texto cifrado, apoyandose en otra clave, en el texto original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales, dependiendo del sistema de cifrado utilizado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado; estas claves se dividen generalmente en dos tipos:

- Las *claves simé*tricas: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.
- Las *claves asimétricas*: son las claves que se usan en el caso del cifrado asimétrico (también llamado cifrado con clave pública). En este caso, se usa una clave para el cifrado y otra para el descifrado.

Esta función es muy útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

Otra de las ramas de la criptología es el *criptoanálisis*, el cual se basa en la utilización de métodos matemáticos permitiendo la reconstrucción de un mensaje cifrado en texto simple.

Generalmente, se distinguen cuatro métodos de criptoanálisis:

- Un ataque de sólo *texto cifrado* consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados;
- Un ataque de *texto simple conocido* consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados conociendo el texto correspondiente;
- Un ataque de *texto simple elegido* consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de textos simples;
- Un ataque de *texto cifrado elegido* consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de los textos simples.

g) Métodos de cifrado de flujo

En el cifrado por flujo de datos se encripta un bit (o byte) de texto plano cada ocasión. El ejemplo más simple de cifrado por flujo de datos es el que consiste en combinar los datos, un bit a la vez, con otro bloque de datos llamado *pad*. Este procedimiento requiere que el pad sea tan largo como el texto plano. Para desencriptar se utiliza el mismo pad y se realiza la operación inversa a la utilizada durante la combinación. Los cifrados por flujo de datos funcionan bastante bien con datos en tiempo real como voz y video, donde en cada momento sólo se conocen pequeñas partes de los datos.

h) Métodos de cifrado en bloque

Los algoritmos de cifrado por bloques operan sobre bloques de tamaño mayor que un bit del texto plano y producen un bloque de texto cifrado; generalmente los bloques de salida son del mismo tamaño que los de la entrada.

El tamaño del bloque debe ser lo suficientemente grande como para evitar ataques de texto cifrado. La asignación de bloques de entrada a bloques de salida debe ser uno a uno para hacer el proceso reversible y parecer aleatorio.
Este tipo de cifrado puede ser considerado como un cifrado por bloques de tamaño 1 bit.

i) Criptografía de clave simétrica

En este modelo, el mensaje original es convertido en un mensaje cifrado que aparentemente es aleatorio y sin sentido. El proceso de encriptación está formado por dos componentes: un algoritmo y una clave. La clave es un valor independiente del texto o mensaje a cifrar. El

algoritmo va a producir una salida diferente para el mismo texto de entrada dependiendo de la clave utilizada.

Una vez cifrado, el mensaje puede ser transmitido. El mensaje original puede ser recuperado a través de un algoritmo de desencriptación y la clave usada para la encriptación.

Los cifrados de clave simétrica tienen varios puntos débiles, y otros fuertes; todos comparten un problema común: para comunicarnos de forma secreta con alguien, es necesario que los dos tengamos una serie de claves. Esto tiene dos problemas:

- Hay que hacer llegar esas claves de una persona a otra de forma segura, y esto es bastante difícil a no ser que nos encontremos en persona.
- Si un grupo de N personas se quiere comunicar entre sí, es necesario contar con claves para cada pareja.

Por otro lado, estos sistemas de cifrado son sencillos de programar, ejecutan muy rápido en cualquier maquina actual. Cifrar un texto grande (digamos un libro de unos cientos de paginas), es una tarea de segundos con cualquier buen algoritmo de cifrado de clave simétrica actual.

j) Criptografía de clave asimétrica

Los algoritmos de criptografía pública se basan en una clave para encriptación y una clave relacionada pero distinta para la desencriptación. Estos algoritmos tienen la característica de que es computacionalmente imposible determinar la clave de desencriptación (clave privada) a partir del algoritmo criptográfico y la clave de encriptación (clave pública).

Los pasos del proceso de encriptación con clave pública son los siguientes:

- Cada sistema genera un par de claves para ser usadas en la encriptación y desencriptación de los mensajes que envíen y reciban.
- Cada sistema publica su clave de encriptación (clave pública). La clave de desencriptación relacionada (clave privada) se mantiene en privado.
- Si A desea enviar un mensaje a B, encripta el mensaje utilizando la clave pública de B.
- Cuando B recibe un mensaje lo desencripta usando su clave privada. Nadie puede desencriptar el mensaje porque sólo B conoce su clave privada.

El problema de las claves asimétricas es que cuando el texto a tratar es largo el proceso de codificación es muy lento. Los protocolos modernos codifican el texto base con una clave simétrica tipo DES o IDEA y utilizan las claves asimétricas para la comunicación de la clave simétrica utilizada. Cuando un texto se codifica mediante una clave simétrica y se envía esta clave codificada con la clave pública del receptor, el resultado se llama "sobre digital".

3.6.3.3. Capa de Internet

Permite la conexión entre diferentes redes a través de procedimientos que permiten que los datos atraviesen las redes interconectadas.

Una de las principales reglas para asegurar un sistema es deshabilitar los servicios TCP/IP no necesarios en cada servidor de la red, de modo que imposibiliten explotar la mayoría de las vulnerabilidades detectadas.

3.6.3.4. Capa de Transporte

Se encarga de facilitar la transferencia de datos de manera fiable entre nodos finales, proporcionando una integridad de los datos y una calidad de servicio previamente establecida.

A este nivel se pueden implementar mecanismos de seguridad que permitan identificar alguna modificación a los paquetes transmitidos.

a) SSL (Secure Shell Layer)

SSL se ejecuta en una capa entre los protocolos de aplicación como http, SMTP, NNTP y sobre el protocolo de transporte TCP de la familia de protocolos TCP/IP.

Permite la confidencialidad debido al cifrado de datos, lo que permite mantener la integridad de los mensajes.

La autenticación de servidores se realiza mediante certificados, mientras que la del cliente puede ser opcional. Aunque proporciona seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos para formar HTTPS.

La Figura 3-5 muestra la ubicación de SSL en el modelo OSI.

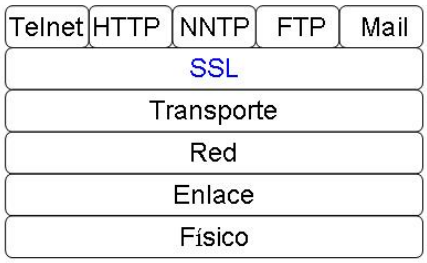

Figura 3-5. Ubicación de SSL

Ventajas:

- Cifra el contenido de las comunicaciones, lo que genera un canal seguro
- Permite autenticar servidores (y clientes)

Limitaciones:

- Sólo protege los datos en tránsito, no en el origen ni destino
- Los ataques web pasan cifrados, pero pasan
- No proporciona un mecanismo de pago seguro
- Dificulta la labor del IDS

3.6.3.5. Capa de Aplicación

La capa de aplicación debe estar protegida por las capas que la preceden, sin embargo existen ataques que no son detectados, como los inmersos en código HTML. De igual manera, puede no prestarse suficiente atención a la seguridad en los desarrollos internos de las entidades.

Una forma de implementar cierto grado de seguridad es el uso de estándares en el desarrollo de aplicaciones e interfaces de usuario final. El uso de productos basados en estándares proporciona la seguridad de que han sido probados, y generalmente se encuentran documentados, para ser empleados de manera correcta.

Uno de los estándares ampliamente difundidos es el desarrollo de aplicaciones basadas en el modelo cliente/servidor, el cual busca minimizar el tráfico en la red al procesar los datos en el lado más rápido.

Dentro de los beneficios de esta arquitectura se pueden mencionar los siguientes:

- Permite integrar aplicaciones que accedan a la misma base de datos de una forma sencilla.
- Permite la separación de las reglas de negocio de las interfaces, lo que genera que cuando éstas se cambien generarán un mínimo impacto sobre los usuarios de las aplicaciones.
- Permite construir nuevas aplicaciones desde los componentes instalados si las reglas de negocio están en servidores de aplicaciones más que en cada aplicación.

La Figura 3-6 nos muestra la interrelación entre las diversas capas del Modelo TCP/IP en relación con las aplicaciones, donde si bien no se detalla capa a capa, si se indican las necesidades de seguridad para cada elemento en las diferentes capas.

Este marco de seguridad [W12] muestra la interrelación entre la Arquitectura del Negocio, la Arquitectura de la Información y la Arquitectura de Tecnología, todas ellas teniendo la seguridad como factor común.

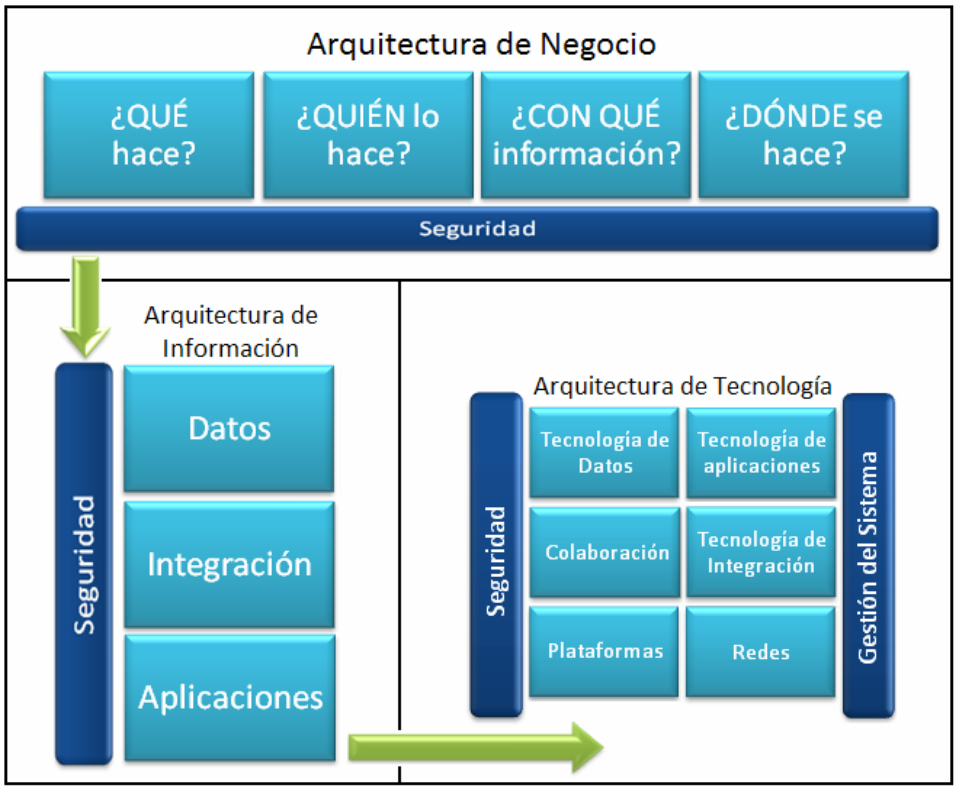

Figura 3-6. Marco de arquitectura de seguridad conceptual de alto nivel[7]

a) Desarrollo de Aplicaciones Web

Existen diversas metodologías para el desarrollo de sistemas, sin embargo el desarrollo de aplicaciones web es relativamente reciente.

Roger S. Presuman dice "Me parece que cualquier producto o sistema importante es merecedor de recibir una ingeniería. Antes de comenzar a construir, lo mejor es entender el problema, diseñar una solución viable, implementarla de una manera sólida y comprobarla en profundidad. Probablemente también se debería controlar los cambios a medida que el trabajo vaya avanzando, y disponer de mecanismos para asegurar la calidad del resultado final. Muchos de los que desarrollan webs no dicen lo mismo; ellos piensan que su mundo es realmente diferente, y que simplemente no se van a aplicar los enfoques de Ingeniería del Software convencionales".

A este respecto se puede resaltar que el desarrollo de una aplicación web no puede seguir las mismas metodologías que el desarrollo de otro tipo de aplicaciones de software ya que requieren un mantenimiento continuo en la gestión de contenidos (diseño visual), navegación dentro de la aplicación, y mecanismos de búsqueda de información, sin embargo una aplicación web pobremente diseñada y desarrollada dará como resultado una alta probabilidad de fallo, y si existe una falla en la aplicación, es muy probable que éste se propague a lo largo de la aplicación.

[7] Marco Huxham. http://es.wikipedia.org/wiki/Arquitectura_de_Seguridad_de_Información_en_la_Empresa

En 1998 surge la Ingeniería Web, realizada por un grupo de profesores de la Universidad de Western, Sydney, quienes conciben a la Ingeniería Web como la aplicación de metodologías sistemáticas, disciplinadas y cuantificables al desarrollo eficiente, operación y evolución de aplicaciones de alta calidad en el World Wide Web.

La Ingeniería web tiene como objetivos[22]

- Gestionar y controlar la complejidad en todo el ciclo de vida
- Soportar efectivamente los tipos de usuario de una aplicación web
- Hacer de los sistemas basados en la web menos una aspiración y más una profesión

La ingeniería Web es multidisciplinaria y comprende contribuciones de diferentes áreas: arquitectura de la información, ingeniería de hipermedia/hipertexto, ingeniería de requisitos, diseño de interfaz de usuario, usabilidad, diseño gráfico y análisis de sistemas, ingeniería de software, ingeniería de datos, indexado y recuperación de información, testeo, modelado y simulación, despliegue de aplicaciones, operación de sistemas, y gestión de proyectos. En el Anexo 4 se describen los desarrollos denominados en dos y tres capas, los cuales son ampliamente utilizados para el desarrollo de aplicaciones web.

El desarrollo web es una mezcla entre la publicación y el desarrollo de software, entre la mercadotecnia y la computación, entre las comunicaciones internas y las relaciones externas, y entre el arte y la tecnología.

Los principios en los que se basa la ingeniería web son:

- Objetivos y requisitos bien definidos
- Desarrollo de un producto en fases
- Diseño y desarrollo sistemático
- Auditoría continua en todo el proceso

Una comparación entre sistemas web simples y sistemas web avanzados se muestran en la Tabla 3-3.

Sistemas web Simples	Sistemas web Avanzados
Fundamentalmente presentan información textual	Páginas web complejas
Los contenidos de información son estáticos	La información es dinámica; cambia con el tiempo y las necesidades de los usuarios
Navegación simple	Dificultad para navegar y encontrar la información
Sistemas aislados	Sistemas integrados con bases de datos, sistemas de planificación, etc.
No requieren de un alto rendimiento	Requieren un rendimiento alto y disponibilidad continua
Desarrollos por una sola persona o por un grupo reducido	Requieren grandes grupos de desarrollo con experiencia en diversas áreas
Se utilizan para distribuir información en aplicaciones no críticas	Se emplean en aplicaciones con contenidos críticos

Tabla 3-3. Comparación de Sistemas Web

Por otro lado, la calidad de las aplicaciones web contempla diversos aspectos, tal como lo muestra la Figura 3-7.

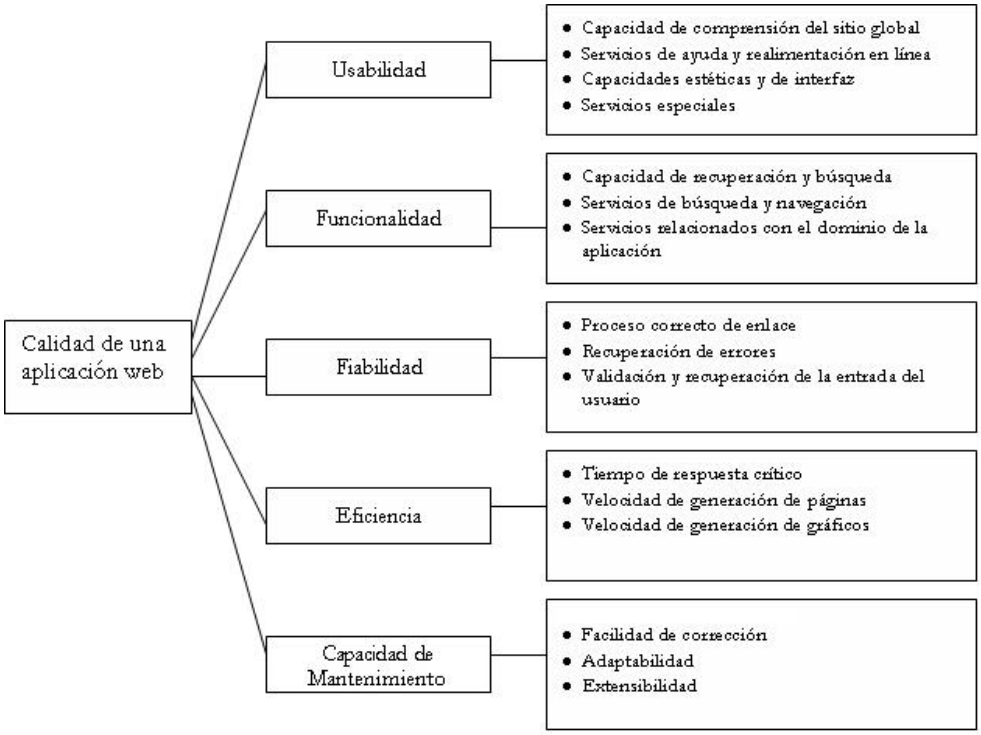

Figura 3-7. Calidad de una aplicación web

b) Vulnerabilidades en Aplicaciones Web

Las vulnerabilidades en aplicaciones web tienen sus particularidades, mismas que deben ser consideradas desde la fase de diseño organizándolas por categorías[W13]. La tabla 3-4 lista las categorías posibles de vulnerabilidades y para cada una de ellas resalta los problemas potenciales que se pueden generar debido a un mal diseño.

Categorización de Vulnerabilidades	Problema Potencial
Validación de Entrada	Ataque ejecutado mediante la inserción de cadenas de texto malicioso en a través de sentencias SQL, campos de formularios, cookies y cabeceras HTTP. Esto incluye ejecución de comandos, cross-site scripting (XSS), SQL injection, y ataques para desborde de buffer (buffer overflow attacks).
Autenticación	Suplantación de identidad, password cracking, elevación de privilegios y acceso no autorizado.
Autorización	Acceso a datos confidenciales o restringidos, ejecución de operaciones no autorizadas.
Administración de configuración	Acceso no autorizado a interfaces de

	administración, alteración de datos de configuración, acceso no autorizado a cuentas de usuario y perfiles de cuentas de usuarios.
Datos sensibles	Acceso a información confidencial
Administración de sesiones	Captura de identificadores de sesión
Ausencia de Encriptamiento	Acceso a datos confidenciales o credenciales de cuenta o a ambos.
Manipulación de parámetros	Ejecución de comandos, elevación de privilegios, Denegación de servicios, etc.
Manejo de Excepciones	Denegación de servicios y acceso a información de detalle en el nivel de sistema.
Auditoría y registro de actividades	Falla para registro de pruebas de intrusión, acciones realizadas por el intruso y dificultades en diagnosticar problemas.

Tabla 3-4. Vulnerabilidades en Aplicaciones Web y problemas potenciales debido a un mal diseño

c) Seguridad en bases de datos

Dado que la información es el activo más importante de las organizaciones, y ésta generalmente se encuentra automatizada en bases de datos, éste es un aspecto realmente importante que debe ser considerado dentro del plan estratégico de seguridad, por lo que para proteger los datos no basta con proteger el servidor de bases de datos, sino que se debe proteger toda la infraestructura que la soporta[22].

Esta área hasta hace algunos años no representaba una mayor complejidad, ya que se manejaban mediante arquitecturas centralizadas y terminales prácticamente dependientes de una unidad central, pero hoy día esta arquitectura ha cambiado debido, en un principio, al concepto cliente-servidor y posteriormente a la descentralización de sites y a los dispositivos móviles que permiten el teletrabajo.

Para generar y mantener un nivel de seguridad en las bases de datos se deben generar perfiles de usuario y de administración, ya que no todos tendrán los mismos privilegios ni accesos a la información contenida en la base de datos. Esto se puede realizar mediante la creación de cuentas de usuario y asignación de contraseñas.

Si bien podemos proteger la información desde el servidor, no debemos olvidar la parte del cliente y sobre todo, cuando ésta viaja a través de la red. Es por ello que a medida de que la tecnología e Internet han ido creciendo, la seguridad en sistemas, pero sobre todo en sistemas web se ha vuelto más compleja.

En la Figura 3-8 podemos ver que con una arquitectura de este tipo es casi imposible acceder directamente a la Base de datos[W13], sin embargo persisten vulnerabilidades que, de manera indirecta, permiten este acceso: inyección de código SQL maligno, manipulación de sesiones y acceso a los logs de transacciones, principalmente.

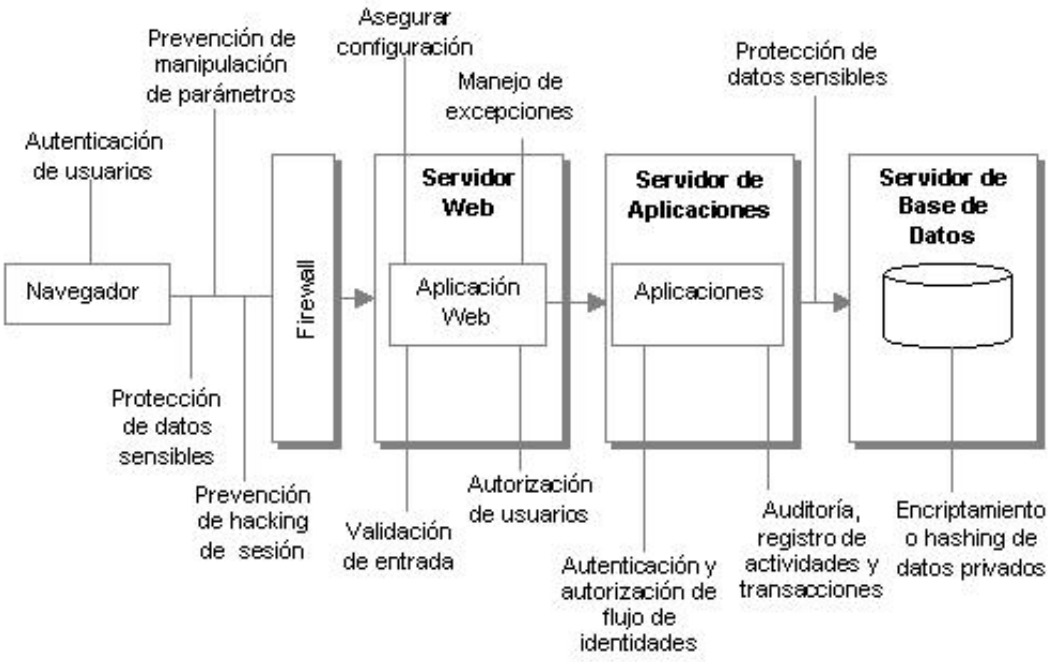

Figura 3-8. Protección a la Base de Datos

- **SQL Injection**

A últimas fechas una vulnerabilidad que se ha venido desarrollando es el SQL Injection, misma que se localiza en el nivel de validación de entradas a la base de datos de una aplicación; se origina en el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.

Consiste en alterar un sistema web mediante sentencias SQL, mismas que se escriben o "inyectan", ya sea en la barra de navegación o en los campos de un formulario de tal manera que el formulario al enviar información hacia la base de datos genera un error, mismo que proporciona información sobre la base de datos que maneja dicho sistema; estos mensajes de error son utilizados para generar un nuevo código y así obtener más información.

Al realizar esta acción de manera cíclica se puede obtener información suficiente que se puede aplicar para dañar o alterar cierta información.

- **Manipulación de Sesiones**

Las aplicaciones web presentan a los diseñadores y desarrolladores muchos desafíos. La naturaleza del protocolo HTTP como un protocolo sin estado implica que el seguimiento de la sesión para cada usuario pasa a ser responsabilidad de la aplicación. Además, la aplicación debe permitir identificar a un usuario usando algún mecanismo de autenticación.

Dado que todas las subsecuentes decisiones de autorización estarán basadas en la identidad del usuario, es esencial que el proceso de autenticación sea seguro y que el mecanismo de manejo de sesión del usuario autenticado esté igualmente bien protegido con mecanismos confiables. Otro desafío se presenta en el paso de datos de entrada y salida a través de redes públicas. Prevenir la manipulación de parámetros y el acceso a datos sensibles son otros de los aspectos a dar prioridad.

- **Acceso al log de transacciones**

Cuando se tiene acceso a los registros de las transacciones realizadas sobre la base de datos se presenta demasiada información relacionada con la estructura y diseño de la base de datos, ya que analizar estos registros se está viendo las tablas y campos contenidos en cada una de ellas.

d) Despliegue de la Aplicación

Durante la fase de diseño del desarrollo de sistemas, se deben revisar los procedimientos y políticas de seguridad dentro de la organización junto con la infraestructura sobre la cual será desplegada la aplicación. Frecuentemente, el entorno de destino no es flexible, por lo que el diseño de la aplicación debe reflejar esas restricciones.

Durante el diseño también se deben tener en cuenta restricciones de protocolo o puertos, o topologías de despliegue específicas a fin de evitar sorpresas posteriormente e involucrar a los miembros de los equipos de red e infraestructura para ayudarnos en el proceso.

La Figura 3-9 nos muestra algunas de las consideraciones que deben tenerse en cuenta durante el proceso de diseño de aplicaciones web.

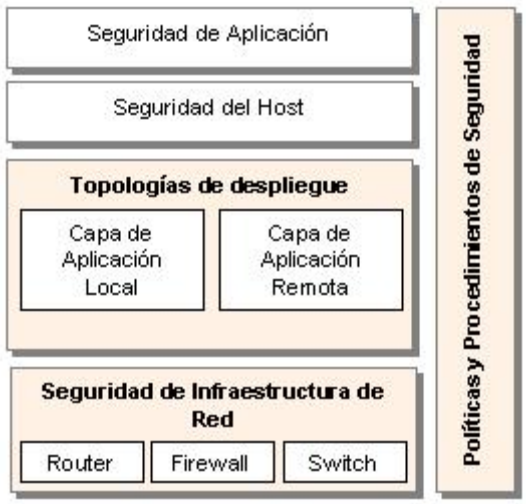

Figura 3-9. Consideraciones en la Capa de Aplicación

- **Políticas y Procedimientos de Seguridad**

Las políticas de seguridad determinan que es lo que les está permitido hacer a la aplicación y usuarios de aplicación; definen las restricciones que determinan qué es lo que no puede hacer una aplicación o usuario.

- **Componentes de infraestructura de red**

Se debe familiarizar con la estructura de red del entorno destino y los requerimientos de seguridad de la red en términos de reglas de filtro, restricciones de puertos, protocolos soportados, etc.

Identificar cómo se ve afectado el diseño y despliegue de la aplicación por las políticas de los firewalls. Puede darse el caso de la existencia de firewalls delante del o los servidores de base de datos. Estos pueden afectar los posibles puertos de comunicación a usar y, por lo tanto, a las opciones de autenticación desde el servidor web a los servidores de aplicaciones y de bases de datos.

- **Topologías de despliegue**

La topología de despliegue de la aplicación y la necesidad de tener una capa de aplicación remota es uno de los puntos clave a considerar e incorporar en el diseño. Si se tiene una capa de aplicación remota, se debe tomar en cuenta cómo asegurar la red entre los servidores para tratar las amenazas como escucha o alteración de datos, por lo que se deben proporcionar mecanismos de protección y aseguramiento de integridad de datos sensibles.

También es importante tener en cuenta los flujos de identidades e identificar las cuentas que serán usadas para autenticación en la red cuando la aplicación conecte a servidores remotos.
Un enfoque común es el uso de una cuenta lo menos privilegiada y el uso de una cuenta espejo o duplicada en el servidor remoto con el mismo password. Otra alternativa es el uso de una cuenta de dominio, la cual facilita la administración, pero con el costo adicional de configurar el uso de la misma en toda la red. La presencia de un firewall o de dominios separados sin relaciones de confianza algunas veces genera que la única opción viable sea el uso de cuentas locales.

- **Intranet, Extranet e Internet**

Cada uno de estos escenarios de aplicación presenta desafíos en su diseño. Los puntos a considerar pueden ser:

- ¿Cómo fluirá la identidad de los llamadores por las múltiples capas de la aplicación para poder obtener acceso a los recursos del back-end?
- ¿Dónde se realizará la autenticación?

3.7. Pruebas de Penetración

Las pruebas de penetración y escaneo de vulnerabilidades actualmente son considerados como una parte importante para la identificación de problemas de seguridad en redes.

El test de penetración[12] es una prueba técnica que se ejecuta en un contexto delimitado (una IP pública, un equipo de red local) en el que se intenta lograr la intrusión explotando vulnerabilidades problemas técnicos y deficiencias de la configuración, con la finalidad de evaluar si un sistema es o no seguro ante un ataque externo.

Para realizar este tipo de pruebas se debe apoyar en el hacking ético, que es una disciplina de la seguridad de redes que se sustenta en el hecho de que para estar protegido se debe conocer cómo operan y qué herramientas utilizan los hackers, además de contar con un grupo de expertos o experto en materia de Sistemas Operativos de redes, Bases de Datos, Programación, Herramientas Antivirus, antispy, etc.

1. Forma de trabajo

1.1. *Pruebas ciegas*. El cliente no proporciona información sobre la infraestructura de comunicaciones ni de sus sistemas. Es quien realiza la prueba el que debe obtener esta información; de esta manera las pruebas son más objetivas y siguen las mismas pautas que si un hacker estuviese intentando atacar a la organización.

1.2. *Pruebas No destructivas*. Se realiza una serie de pruebas no destructivas desde dentro y fuera de la organización utilizando técnicas similares a las que un hacker puede usar para acceder a la red.

1.3. *Documentar las vulnerabilidades***.** Las vulnerabilidades encontradas, así como las medidas precautorias deben ser entregadas en un informe al finalizar la revisión.

2. Pasos del Test

2.1. *Elección de Objetivos***.** Se debe elegir el punto de ejecución del test.

2.2. *Inventariar Activos de la Empresa***.** Se debe buscar dónde hay una puerta de entrada. Para ello se analizan los activos de la empresa que estén visibles y disponibles, es decir, qué servicios y/o servidores están a disposición: servidores web, servidores de conexiones VPN, servidor de correos, servidor de archivos

2.3. *Recolección de Información***.** La información acerca de la dirección de red de destino, ala que generalmente se llama huella digital, debe obtenerse antes de realizar un ataque. Esto incluye recabar la máxima cantidad posible de información acerca de la infraestructura de comunicaciones de red: direcciones IP, nombres de dominio, protocolos de red, servicios activos, arquitectura del servidor, …

Al obtener el nombre de dominio de una organización un pirata informático puede conocer el rango de direcciones IP pertenecientes a la organización, así como su división en subredes consultando las bases públicas que administran las direcciones IP y los nombres de dominio (iana, ripe, arin).

Además, puede utilizar motores de búsqueda para recabar información acerca de una organización como productos principales o incluso los nombres de sus empleados.

2.4. *Análisis***.** Una vez conocida la topología, se puede analizar una red a fin de determinar IPs activas, puertos abiertos, sistemas operativos y configuraciones de servidores. También se puede realizar un análisis de vulnerabilidades y, lo más grave, un password cracking.

Los siguientes pasos son lo que realiza un hacker en un sistema objetivo, por lo que es recomendable llevarlos a cabo con extremo cuidado y apoyados por los administradores de los sistemas a fin de evitar un mal uso de la información recolectada y eliminar las vulnerabilidades lo más pronto posible.

2.5. *Intrusión*. Cuando se conoce la infraestructura de comunicaciones se está en posibilidades de realizar la intrusión. Para ello se debe acceder mediante cuentas válidas en los equipos que ha catalogado como objetivo.

2.6. *Aumento de privilegios*. Cuando se obtiene uno o más accesos a la red mediante cuentas con niveles de protección bajos, se intenta aumentar los privilegios con el objetivo de llegar a obtener los mismos que la cuenta root.

Si se llega a este nivel, quiere decir que tenemos un alto grado de vulnerabilidad y que estamos ante un ataque de suplantación de identidad, y que debido a las relaciones de confianza indicadas en los servidores toda nuestra infraestructura y sistemas están comprometidos.

2.7. *Eliminación de rastros*. Una vez que se ha obtenido suficiente control sobre la red, se deben borrar las evidencias del acceso mediante la eliminación de archivos creados y los de registro de los equipos a los cuales se conectó.

3. Resultados

Los resultados obtenidos deben ser documentados y entregados a los responsables de la seguridad a fin de subsanar las vulnerabilidades encontradas.

Se deben detallar todas las pruebas realizadas especificando el objetivo, los resultados obtenidos, las recomendaciones de solución a cada falla encontrada y clasificar los problemas de seguridad de acuerdo con su nivel de riesgo.

4. Implementación de mecanismos de seguridad mediante un Sistema de Gestión de Seguridad de la Información

La seguridad de la información se ha convertido en un factor cada vez más importante para las organizaciones, por lo que es necesario contar con mecanismos que permitan reducir el nivel de riesgo al que se está expuesto; la seguridad a implementar engloba la infraestructura de operación con que se cuenta, la cual está integrada por equipamiento técnico, software, procedimientos y personal involucrado en el manejo de la información cuyo objetivo es preservar su integridad, confidencialidad y disponibilidad.

El nivel de seguridad de la organización, en este caso el de la División de Estudios de Posgrado de la Facultad de Economía, debe estar estipulado en un documento denominado *Política de Seguridad*; en él se cubren aspectos relacionados con el uso de los elementos operativos, mismo que van desde un nivel sencillo como son las reglas de acceso a datos o a la infraestructura, hasta procedimientos y normas de operación específicos.

Para lograr el nivel de seguridad deseado en una organización y plasmarlo en la política de seguridad, se deben llevar a cabo dos procesos complementarios: por un lado el estudio del estado actual de la seguridad, y por el otro la implantación o mejora de la seguridad. Esto permitirá implantar mejoras y subsanar vulnerabilidades en la organización.

El estudio del estado actual de seguridad de la organización es un proceso que debe incluir una serie de estudios técnicos que se apoyen en técnicas que utilizan los atacantes buscando vulnerabilidades y agujeros de seguridad (conocido como "hacking ético"); mediante este estudio podemos identificar las necesidades concretas de la organización para posteriormente implantar las medidas correctivas necesarias y así tener como producto una política de seguridad específica y válida para la organización.

La implementación o mejora de la seguridad es un proceso que debe apoyarse en estándares que indiquen a dónde se desea llegar. La norma ISO/IEC 17799 especifica las exigencias necesarias para establecer, implantar, explotar, controlar, revisar, documentar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en el contexto de una organización que implica riesgos de negocios, aunque también puede ser implementada en una entidad académica como en este caso, ya que constituye un elemento de referencia para ayudar a la organización a establecer sus objetivos particulares en torno a la seguridad.

Esta norma proporciona un marco de referencia a lo que se debe hacer para implementar un Sistema de Gestión de Seguridad de la Información dentro de cualquier organización, sin embargo no dice cómo hacerlo, por lo que ese es el trabajo que se desarrolla en el presente capítulo.

Un paso previo al desarrollo e implementación de la metodología es el conocimiento de la organización cuyo estado de la seguridad se va a evaluar, por lo que a continuación se da una breve explicación del entorno de la División de Estudios de Posgrado de la Facultad de Economía.

4.1. Entorno de la División de Estudios de Posgrado de la Facultad de Economía

La División de Estudios de Posgrado de la Facultad de Economía (DEP-FE) cuenta con una planta docente con amplia experiencia profesional, cuyas labores primordiales son la docencia, la investigación y la difusión de la Economía. Físicamente se encuentra ubicada en el Edificio "B" de la Facultad de Economía, el cual comparte con la División del Sistema de Universidad Abierta, el área de Educación Continua y las Aulas multimedia de la propia Facultad, así como con el Auditorio "Narciso Bassols" y el Centro de Desarrollo Empresarial (CEMPE).

La mayoría de la planta docente se ubica físicamente en los cubículos del edificio "B" y en su minoría en cubículos del Edificio "C", lo que anteriormente se denominaba Unidad Académica de los Ciclos Profesionales y del Posgrado (UACPyP).

Respecto a la infraestructura y ubicación, se pretende que para el año dos mil diez, la DEP-FE cuente con su propio edificio albergando oficinas administrativas, cubículos y áreas académicas, aulas y biblioteca que ayuden a continuar con su labor docente y de difusión.

En lo relativo a las áreas de trabajo, la DEP-FE se encuentra organizada como lo muestra la Figura 4-1.

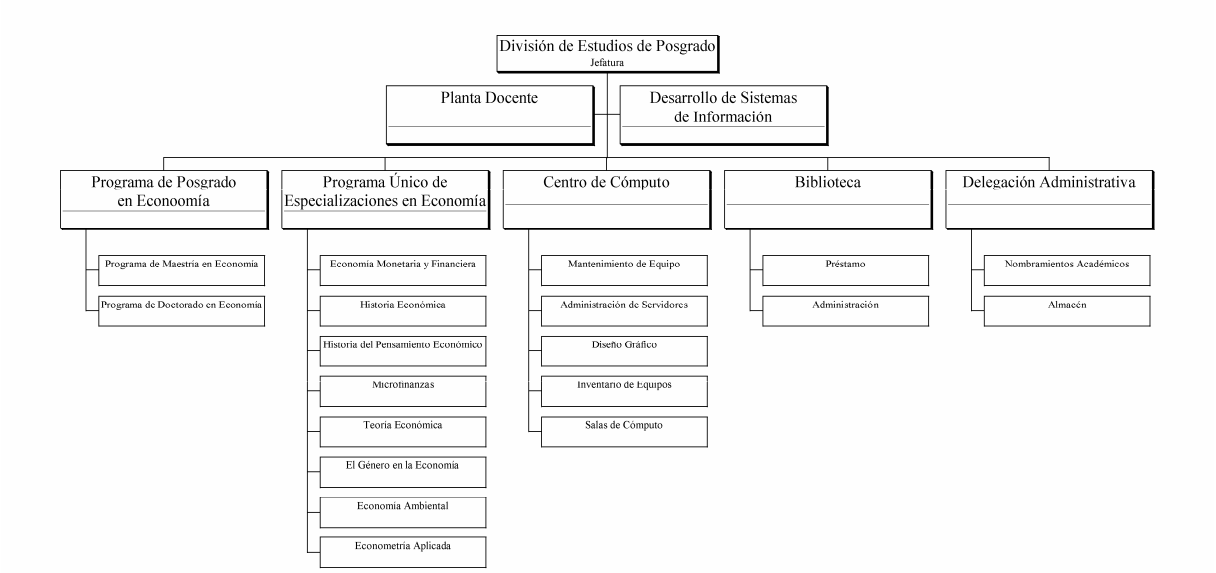

Figura 4-1. Áreas de Trabajo de la División de Estudios de Posgrado de la Facultad de Economía

4.1.1. Misión

La División de Estudios de Posgrado de la Facultad de Economía tiene como Misión la formación de profesionistas para desempeñarse en niveles de alta dirección tanto en el sector público como en el privado, en organizaciones sociales o en organismos no gubernamentales, impulsando a su vez el desarrollo de habilidades docentes.
Los esfuerzos se encaminan a formar profesionistas capaces de realizar investigación en temas de frontera que los coloquen entre los mejores del mundo acercándolos a profesionistas e investigadores de renombre internacional a fin de compartir el conocimiento y experiencia adquiridos.

4.1.2. Funciones

La Jefatura de la División de Estudios de Posgrado es la encargada de planificar, evaluar y coordinar las actividades académicas y administrativas realizadas por los docentes y el personal administrativo de la División de Estudios de Posgrado (DEP).

Conlleva la administración de actividades académicas y de difusión, entre las que se encuentran:

- Coordinación de actividades académicas de profesores.
- Generación de la planta académica semestral.
- Organización de eventos académicos.
- Ejecución de convenios con entidades externas a la UNAM.

De igual manera, realiza el intercambio de información con las áreas sustantivas de la Facultad de Economía, principalmente las áreas administrativas y contables.

4.1.3. Programas Académicos

La División de Estudios de Posgrado alberga en su infraestructura física al Programa de Posgrado en Economía y al Programa Único de Especializaciones en Economía.

4.1.3.1. Programa de Posgrado en Economía

El Programa de Posgrado en Economía (PPE) cuenta con dos programas: Maestría y Doctorado. La Maestría pertenece al Padrón Nacional de Posgrados de alto nivel y el Doctorado forma parte del Programa Integral de Fortalecimiento del Posgrado.

La División de Estudios de Posgrado, al ser la primera institución en proporcionar estudios de posgrado en ésta área, es la sede con mayor número de matrícula estudiantil, así como con el mayor número de tutores. A partir del 2002, año en que se integró el Programa de Posgrado en Economía ésta División colabora con otras tres entidades académicas, las cuales le siguen en tamaño e infraestructura en el siguiente orden: el Instituto de Investigaciones Económicas, la Facultad de Estudios Superiores "Aragón", y la Facultad de Estudios Superiores "Acatlán".

En el año 2007 se incorporó a este programa la Universidad Técnica Particular de Loja, Ecuador, como parte de un convenio signado entre dicha Universidad y la UNAM, y para el año 2008 se incorporó la Cámara de Diputados con 14 estudiantes, también al programa de Maestría en Economía mediante otro convenio.

A fin de llevar a cabo sus actividades administrativas, este programa se apoya en el Área de Servicios Escolares de la DEP, la cual se encarga de brindar información, orientación y servicios a los interesados en ingresar a la Maestría o Doctorado del PPE, desde su postulación hasta la obtención del grado, lo cual implica

- Publicar la Convocatoria de ingreso, tanto para la Maestría como para el Doctorado.
- Registrar aspirantes.
- Aplicar exámenes de selección.
- Registrar alumnos aceptados.
- Dar seguimiento a los alumnos matriculados: ingreso, avance y exámenes de grado.

De igual manera, se encarga de proporcionar la información pertinente a las instancias académico-administrativas que lo requieran así como de proporcionar apoyo de carácter administrativo a los profesores del posgrado y a la Coordinación del PPE.

4.1.3.2. Programa Único de Especializaciones en Economía

La Especialización es el nivel de estudio de Posgrado cuyo objetivo es profundizar en el conocimiento de una temática específica de la Economía. Comprende, con este enfoque, ahondar en la cognición, el aprendizaje básico de los principales enfoques teóricos hasta sus desarrollos más recientes y el manejo adecuado de los métodos matemáticos y econométricos de uso más generalizado en la especialización concreta.

Este programa fue autorizado en el año 2004 e implementado en el 2005 con seis especializaciones, incorporando dos más en el 2008.

El propósito general del Programa es profundizar y ampliar los conocimientos y destrezas que requiere el ejercicio profesional en diversas áreas de la Economía mediante la formación especializada en temas específicos, de tal manera que en el transcurso de un año el alumno adquiera el conocimiento y las herramientas necesarias para desempeñarse como especialista en las temáticas que ofrece el Programa.

A la fecha la planta de profesores con que cuenta posee una amplia experiencia académica en la materia correspondiente, así como en el ejercicio de la profesión.

4.1.4. Centro de Cómputo

El Centro de Cómputo tiene como misión brindar a los estudiantes, académicos y personal administrativo de la DEP-FE las asesorías y servicios de infraestructura necesarios para realizar sus actividades académicas y laborales, utilizando como herramienta principal los medios electrónicos computacionales.

4.1.5. Biblioteca

La Biblioteca "Ramón Ramírez Gómez" es una de las más importantes de su género en el país, ya que es proveedora de información especializada en Economía y materias específicas como la Economía internacional, Economía política, Economía financiera y Econometría, por mencionar algunas.

Ofrece préstamo en sala, externo e ínter bibliotecario; catálogo para búsqueda de los materiales (Aleph) y servicio de fotocopias.

Tiene como objetivos atender las necesidades y demandas de información de la comunidad, proporcionar servicios eficientes y oportunos, y apoyar las actividades de investigación que establecen los planes y programas de estudio del Programa de Posgrado en Economía de la UNAM, que incluyen al Instituto de Investigaciones Económicas, FES-Aragón, FES-Acatlán, la División de Estudios de Posgrado de la Facultad de Economía, y la Licenciatura de la FE, así como a la comunidad universitaria y al público en general.

4.1.6. Delegación Administrativa

Es el área encargada de las contrataciones de profesores de tiempo completo, ayudantes de profesor y técnicos académicos adscritos a la DEP-FE, principalmente.

Es responsable de tramitar los asuntos relacionados con Licencias y Sabáticos, en coordinación con el H. Consejo Técnico de la Facultad, ante la Dirección General de Personal.

También se responsabiliza de la administración del presupuesto asignado a la DEP-FE a fin de cubrir sus necesidades de mobiliario, papelería, suministros, organización de eventos académicos, difusión de la cultura, apoyo a profesores para viáticos, entre otros.

4.1.7. Personal en la División de Estudios de Posgrado

El personal adscrito a la División de Estudios de Posgrado está conformado como se indica en la Tabla 4-1:

Tipo de Personal	Frecuencia
Investigador de Carrera	1
Profesores de Carrera	41
Técnicos Académicos	9
Personal Académico-Administrativo	4
Personal de Confianza	4
Personal de Base	28
Ayudantes de profesor	30-35

Tabla 4-1. Personal Adscrito a la DEP-FE

Las contrataciones de ayudantes de profesor varían cada semestre, ya que éstas se realizan en base a las solicitudes de los profesores de carrera, las cuales están asociadas a las asignaturas que se imparten por semestre.

Cada miembro del personal es dotado con un equipo de cómputo de escritorio para realizar sus actividades; estos equipos se pueden incrementar debido a que los profesores de carrera adscritos a la DEP-FE tienen bajo su responsabilidad proyectos de investigación mediante los cuales pueden adquirir equipos y accesorios de cómputo (escáner, impresoras, etc.), lo que les permite actualizar sus equipos de cómputo y crear pequeñas áreas de trabajo con la posibilidad de integrar a sus ayudantes, estudiantes y becarios del Posgrado.

4.1.8. Ubicación Física de la División de Estudios de Posgrado

La División de Estudios de Posgrado se encuentra ubicada en el Edificio "B" de la Facultad de Economía, el cual comparte con la División del Sistema de Universidad Abierta, el área de Educación Continua y las aulas multimedia de la propia Facultad, así como con el Auditorio "Narciso Bassols" y el Centro de Desarrollo Empresarial (CEMPE).

Algunos profesores de carrera se encuentran ubicados en el Edificio "C" de la Facultad de Economía, lo que anteriormente se le denominaba Unidad Académica de los Ciclos Profesionales y del Posgrado (UACPyP), aunque la mayoría se ubica en el Edificio "B".

Respecto a la infraestructura y ubicación, se pretende que para el 2010, la DEP-FE cuente con su propio edificio albergando oficinas administrativas, cubículos y áreas académicas, aulas y biblioteca que ayuden a continuar con su labor docente y de difusión.

4.1.9. Infraestructura de comunicaciones

La División de Estudios de Posgrado, al formar parte de la Facultad de Economía no tiene una infraestructura de comunicaciones independiente; es el Centro de Informática de la Facultad de Economía (CIFE) el encargado de la administración de la red existente; sin embargo las actividades de asignación y resguardo de equipo de cómputo, actualización de vacunas, desarrollo de sistemas propios y administración de los servidores del posgrado son atendidos por personal del Centro de Cómputo y de la Jefatura de la DEP-FE.

4.1.9.1. Componentes de la Red

La red de la Facultad de Economía se compone de poco más 800 equipos distribuidos en salones de cómputo, salas de usuarios y en las diversas áreas administrativas, docentes y de investigación de las Divisiones de Estudios Profesionales y de Posgrado.

Cuenta también con un servidor de correo, tres servidores web, dos servidores de aplicaciones y dos servidores Proxy.

La División de Estudios de Posgrado, por sí misma, cuenta con poco más de 300 equipos de cómputo distribuidos en áreas académicas, administrativas y de servicio, un servidor web, y un servidor para la plataforma educativa Moodle.

Aún cuando se maneja un número considerable de equipos, el entorno de red está configurado para que el usuario pueda visualizar toda la red y no existe ninguna medida que regule que un usuario comparta sus datos o impresora con otros usuarios.

4.1.9.2. Conexiones hacia el exterior

El enlace hacia el anillo de red (RedUnam) se lleva a cabo a través de un backbone Gigabit mediante un switch E7 de Enterasys. Las conexiones del switch cabecera al primer switch se realizan a través de fibra óptica a 1000 Mbs; para ello se cuenta con 20 switches 10/100 de 24 y 48 puertos E1 puestos en cascada, si es el caso, a través de fibra o de stacks de cobre.

Hasta el momento se ha instalado cableado estructurado (categoría 6 y 5e) para 1000 servicios, aunque la infraestructura puede soportar hasta 1200 servicios. Cabe mencionar que la Facultad cuenta con 44 puertos con conexión de cobre a Gigabit para el proyecto de Internet 2 (I2), los cuales a la fecha sólo han sido utilizados para la transmisión de videoconferencias.

Las conexiones hacia el edificio "B" de la DEP-FE se realiza a través de un cable de fibra a 1000Mbs.

4.1.9.3. Servidores Proxy

Es importante destacar que para sus comunicaciones la Facultad de Economía cuenta con 508 IP´s homologadas divididas en dos segmentos. Para subsanar la falta de IP´s homologadas se cuenta con dos servidores Proxy, los cuales funcionan con un rango de direcciones IP definido y configurados sólo con el número necesario de puertos abiertos.

4.1.9.4. Servidores de Aplicación

La Facultad de Economía cuenta con servidores de aplicación que tienen instalados los programas de misión crítica relacionados con el control escolar de la División de Estudios Profesionales y otros dos de tipo administrativo basados en web a través de aplicaciones. Estos servidores corren sus aplicaciones utilizando Coldfusion y PHP para la programación y acceso a bases de datos diseñadas en SQL Server. El servidor se encuentra detrás de un firewall para su protección y montado sobre Windows 2003 Server, el cual cuenta con procesadores Xeon a 2.8 Ghz con 1Gb en memoria RAM y 300Gb de capacidad en disco duro.

En la DEP-FE se cuenta con aplicaciones propias desarrolladas ad-hoc a sus necesidades: registro de productividad académica de los profesores e investigadores, administración escolar, nombramientos académicos y de actividades propias de la Jefatura de la División, además de las proporcionadas por la plataforma educativa Moodle.

Las aplicaciones propias se encuentran desarrolladas en PHP como lenguaje de programación y una base de datos montada en PostgreSQL ver 8.0.2. Este servidor no se encuentra protegido por un firewall.

4.1.9.5. Firewall de la División de Estudios Profesionales

Consiste en un CheckPoint FireWall-1, el cual está configurado para:

- Protección contra ataques con conocimiento de las aplicaciones
- Control de acceso basado en Statefull Inspection
- Escalable con una variedad de productos Check Point y OPSEC
- Gestión especializada para una eficiencia máxima de manera que se prohíben todos los servicios y sólo se habilitan los necesarios (postura de negación preestablecida)

Este firewall permite la protección de los niveles de red y aplicaciones, además de control de accesos, seguridad de contenidos, autentificación y conversión de dirección de red (NAT) integrada

4.1.9.6. Tráfico de la red

El tráfico que circula por la red interna de la Facultad de Economía se muestra en la Tabla 4-2.

Tipo de Táfico	Porcentaje
Address Resolution Protocol	38.24
Logical-Link Control	13.37
Internetwork Packet eXchange	19.80
Internet Protocol	26.14
Internet Protocol Version 6	2.18
MDS Header	0.25
Data	0.02

Tabla 4-2. Tráfico interno de la Facultad de Economía

4.2. Metodología para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI)

La seguridad de la información es necesaria ya que las organizaciones, su infraestructura de comunicación y sistemas de información se enfrentan día a día con amenazas que provienen de diversas fuentes.

Esta metodología establece una serie de etapas a realizar con la finalidad de cubrir diversos aspectos de seguridad en una organización[12] y [24]; hace referencia a la evaluación de riesgos como un paso importante en la gestión de la seguridad.

Mediante la evaluación de riesgos se desarrollarán los controles necesarios para la organización en cuestión así como el cálculo de

- *El impacto potencial de una falla de seguridad*, teniendo en cuenta las consecuencias por una pérdida de confidencialidad, integridad o disponibilidad de la información.
- *La probabilidad de ocurrencia de dicha falla*, considerando las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para administrar los riesgos asociados a la seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.

En la Figura 4-2 se presentan las etapas a realizar[12], donde en cada fase se e genera un documento o serie de documentos que indican el estado de seguridad de la organización, tanto actual como al que se desea llegar.

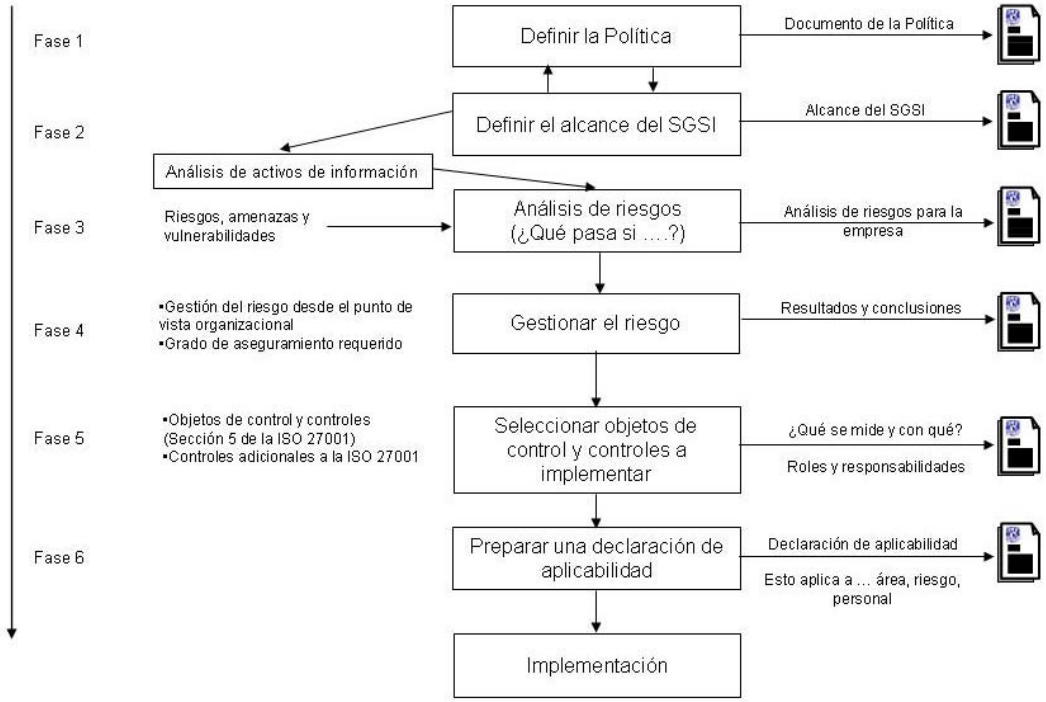

Figura 4-2. Metodología de Seguridad de la Información

Aunque pareciera que con la implementación se termina el proceso, esto es totalmente erróneo, ya que la seguridad es un proceso en constante adaptación, por lo que es importante realizar revisiones periódicas de los riesgos de seguridad y de los controles implementados, ya que con el tiempo cambian tanto las amenazas y vulnerabilidades como los requerimientos y necesidades de las organizaciones.

4.3. Desarrollo de un Sistema de Gestión de Seguridad de la Información para la División de Estudios de Posgrado

La Norma ISO/IEC 17799 proporciona recomendaciones de buenas prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran).

En el Capítulo 1 se menciona que la seguridad no es un producto, es un proceso y por lo tanto debe ser gestionada de manera permanente, por lo que las siguientes fases deben realizarse de manera cíclica buscando siempre la mejora y adaptación a las nuevas tecnologías.

4.3.1. Fase 1. Definir la Política

4.3.1.1. Planteamiento

Las tecnologías de información tuvieron un desarrollo masivo a inicios de la década de los 90, sin embargo no todas las organizaciones estaban preparadas para ello y en muchos casos se fueron adaptando conforme las exigencias de sus colaboradores, clientes o pares les fueron requiriendo.

La Facultad de Economía no estuvo ajena a esta problemática, ya que a mediados de los noventa no contaba con la infraestructura de comunicaciones requerida.

Fue hasta el año 2002 que se inició un proyecto que abarcara las diversas áreas de la Facultad de Economía dotando de infraestructura de comunicaciones en una primera etapa a profesores y salones de cómputo para en una segunda etapa cubrir las áreas administrativas.

Al realizar esta adecuación de infraestructura, con un presupuesto limitado y sin considerar capacitar a los usuarios se tuvo como consecuencia la falta de previsión de problemas como son la capacitación del personal que utiliza el equipo, la protección individual de los equipos, el mantenimiento de los mismos y, sobre todo, la revisión de su utilización.

De igual manera el crecimiento de la interrelación de académicos con pares de otras instituciones y el incremento en la investigación que se realiza requiere de la creación de un plan de seguridad que subsane las deficiencias de la infraestructura actual y que a su vez pueda ser administrado por personal propio de la DEP-FE, eliminando la dependencia y centralización de funciones.

La DEP-FE inició en el 2005 el desarrollo de sistemas de información que sirvieran de apoyo a la gestión de actividades académico-administrativas, principalmente para la productividad de la planta académica, el seguimiento de alumnos inscritos en alguno de los programas de posgrado, y las actividades propias de la Jefatura de esta División.

4.3.1.2. Hipótesis

La implementación de un Sistema de Gestión de Seguridad de la Información minimiza el riesgo de pérdida de información y ataques a la infraestructura de comunicaciones de cualquier entidad derivado de algún ataque, generando así un mayor grado de confiabilidad en la información y confianza por parte de sus usuarios.

4.3.1.3. Objetivos

i. Proteger los servidores de aplicaciones contra usuarios externos así como contra cualquier contingencia de origen natural, física o personal que pudiese surgir dentro y fuera de las instalaciones de la entidad académica.

ii. Proteger la información contenida en los servidores contra ataques de cualquier índole, así como contar con los respaldos necesarios y suficientes para restaurar el ambiente de trabajo en caso de alguna contingencia.

iii. Definir un SGSI que sea capaz de identificar los aspectos de seguridad más relevantes en la DEP-FE manteniendo la seguridad en un nivel mínimo aceptable.

4.3.1.4. Definición de la Política

Una política de seguridad debe contener un objetivo general, la importancia de la infraestructura de comunicaciones y de las tecnologías de la información para la entidad, el periodo de validez de esta política, los recursos con que se cuenta, y los objetivos específicos de la entidad (ver 3.1).

La política definida para la DEP-FE está orientada para proteger la integridad, confidencialidad y disponibilidad de la información a fin de proporcionar la continuidad en las operaciones.

Esta política proporciona una visión global de los aspectos considerados estratégicos y así brinda seguridad a la información manejada en esta dependencia universitaria. Cabe aclarar que esta política es el resultado del análisis de riegos y selección de controles implementados en los activos a proteger dentro del alcance de este SGSI.

4.3.2. Fase 2. Definir el alcance y limitaciones del SGSI

En esta primera aproximación a la implementación de un SGSI, se cubrirán aspectos relacionados con la Seguridad Lógica de la entidad.

4.3.2.1. Alcance

i. Gestión de Comunicaciones y Operaciones
Se establecerán las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidentes.

Se implementará la separación de funciones cuando así se requiera a fin de reducir el riesgo por el uso de manera negligente o mal uso deliberado del o los sistemas de información.

ii. Control de Accesos
El acceso a la información y a los procesos de operación deberá estar controlada en base a los requerimientos de la seguridad y la lógica del negocio, es decir, dándole un enfoque específico considerando las actividades propias de la entidad académica.
Para este aspecto se deben considerar las políticas de gestión, autorización y difusión de la información.

iii. Desarrollo y Mantenimiento de Sistemas de Información
Esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por la propia División de Estudios de Posgrado de la Facultad de Economía. El diseño e implementación de los procesos de negocio que apoyen la aplicación o servicio proporcionado pueden ser cruciales para la seguridad.

4.3.2.2. Limitaciones

Los límites del alcance de este SGSI se encuentran determinados por:

- Tamaño de la entidad académica.
- Ubicación física de la entidad académica
- Dependencia de la administración de la red por parte del CIFE
- Personal capacitado
- Renuencia de los usuarios
- Cotos de poder
- Reglamentos internos

4.3.2.3. Análisis de Activos de la Información

Una vez delimitado el alcance, se procede a realizar un análisis preliminar del estado de seguridad que guarda esta entidad académica y posteriormente definir un plan de acción, así como su implementación mediante políticas, procesos y herramientas tecnológicas que permitan garantizar la seguridad requerida.

En el Anexo 1 se presenta una primera aproximación a la norma UNE-ISO/IEC 17799 mediante un cuestionario estándar aplicado a la División de Estudios de Posgrado de la Facultad de Economía [24]. De este cuestionario se derivaron las siguientes etapas en el desarrollo:

a) Recopilación de documentación existente

Se realizó la recopilación de toda documentación existente referente a la seguridad de la información, dentro de la cual encontramos:

- Documentación de Políticas de Seguridad (Inexistente).

- Normas y Procedimientos de las Políticas de operación, ya sea administrativos o técnicos (Deficientes).
- Informes de evaluación de riesgos (Inexistente).
- Planes de administración de riesgos (Inexistente).
- Documentos que indiquen la existencia de controles de seguridad y su gestión; por ejemplo informes y pistas de auditoria, informes de incidencias, etc. (Inexistente)
- Documentación de Sistemas de Información desarrollados (No actualizada)

Lamentablemente, después de la puesta en operación de la infraestructura de comunicaciones de la DEP-FE no se han realizado actividades de seguimiento o auditorías al uso de la red o documentación de los sistemas desarrollados para cubrir las necesidades de esta División sin embargo, consciente de la importancia de implantar políticas de seguridad, personal del Centro de Cómputo de la DEP-FE ha trabajado en la normatividad de los siguientes aspectos:

- Registro de equipos nuevos
- Solicitud de servicios de cómputo (instalación de equipo de cómputo, software o impresoras; antivirus, …)
- Registro de asignación de equipo de cómputo y componentes
- Campañas antivirus y mantenimiento preventivo
- Lineamientos para el uso de las salas de trabajo (préstamo de equipo)
- Solicitud para uso de la plataforma educativa Moodle
- Alta de cursos en la plataforma educativa Moodle

Aunque representan un buen inicio para gestionar la seguridad, estos lineamientos no cubren totalmente las necesidades particulares de la DEP-FE.

b) Identificación de activos

La identificación de activos nos ayuda a conocer y estar ciertos en cuanto a lo que posee la DEP-FE en los procesos de generación, transferencia y almacenamiento de la información, así como los servicios que puede proporcionar a través de éstos.

Para poder realizar una identificación y selección de activos se debe comprender la fuente y naturaleza de las vulnerabilidades y amenazas, sin menospreciar cualquiera de ellas.

En este caso particular, se puso especial atención a los activos que se considera están directamente relacionados con el desarrollo de sistemas de información, ya que éstos son los que proporcionan los servicios de disponibilidad de la información, además de los asociados a las comunicaciones y operaciones de los sistemas, como es el caso de los servidores y equipos de escritorio que se utilizan para el ingreso a los sistemas de información de operación diaria.

De igual manera la evaluación se enfocó en la infraestructura física de de la DEP-FE, ya que al compartir instalaciones se incrementa el número de personas que tienen acceso a esta institución extendiendo a su vez el riesgo de ataque o pérdida de información.

En la Tabla 4-3 se encuentran agrupados los activos identificados, así como el responsable o área en la cual se encuentra.

	Infraestructura física	Responsable
1	Edificio / Construcción	Facultad de Economía
2	Mobiliario	Registrado por el área de bienes y suministros; resguardado por cada usuario

	Infraestructura de comunicaciones	Responsable
3	Switch	Centro de Informática de la Facultad de Economía
4	Hub	Centro de Informática de la Facultad de Economía
5	Ruteador	Centro de Informática de la Facultad de Economía
6	Conexión de fibra a DGSCA	Centro de Informática de la Facultad de Economía
7	Servidores	CIFE y Centro de Cómputo de la DEP-FE
8	Equipo de Videoconferencia	Centro de Informática de la Facultad de Economía
9	Firewall	Centro de Informática de la Facultad de Economía

	Hardware	Responsable
10	Equipo personal (Monitor, CPU, Teclado, mouse)	Administrado por el Centro de Cómputo de la DEP-FE y resguardado por cada usuario
11	LapTop	Centro de cómputo
12	Impresora de matriz	Cada área o usuario responsable
13	Impresora láser	Cada área o usuario responsable
14	Impresora a color	Diseño gráfico
15	Impresora doble carta	Cada usuario responsable
16	UPS	Cada usuario responsable
17	Proyector de datos (mini cañón)	Centro de cómputo
18	Tarjetas inalámbricas	Centro de cómputo y cada usuario responsable
19	Teléfono inalámbrico	Jefatura de la DEP-FE

	Software	Responsable
20	Sistema Operativo	Centro de Cómputo
21	Suite de escritorio	Centro de Cómputo
22	Paquetes estadísticos	Centro de Cómputo
23	Manejadores de Bases de Datos	Centro de Cómputo
24	Antivirus	Centro de Cómputo
25	Antispam	Centro de Cómputo
26	Herramientas de Desarrollo	Centro de Cómputo y desarrollador

	Servicios Proporcionados	Responsable
27	Servidor de correo	Centro de Informática de la Facultad de Economía
28	Servidor de la Página web de la DEP-FE	Administrador del servidor - Centro de Cómputo
29	Servidor de las Bases de Datos de la DEP-FE	Administrador del servidor - Centro de Cómputo
30	Servidor de la plataforma educativa Moodle	Administrador del servidor - Centro de Cómputo
31	Servidor de Biblioteca	Centro de Informática de la Facultad de Economía
32	Fotocopiado	Delegación Administrativa de la DEP-FE

	Sistemas de Información	Responsable
33	Sistema de Información de la Jefatura de la DEP-FE	Desarrollador de sistemas
34	Sistema de Información de la Planta Académica de la DEP-FE	Desarrollador de sistemas
35	Sistema de alumnos de Doctorado en Economía	Desarrollador de sistemas
36	Sistema de alumnos de Maestría en Economía	Desarrollador de sistemas
37	Sistema del Programa Único de Especializaciones en Economía	Desarrollador de sistemas
38	Sistema de la Coordinación del Programa de Posgrado en Economía	Desarrollador de sistemas

39	Sistema de Inventarios	Desarrollador de sistemas
40	Código Fuente	Desarrollador de sistemas
41	Bases de Datos	Administrador del servidor – Desarrollador de sistemas

	Documentación	**Responsable**
42	Oficios de la Jefatura	Jefatura de la DEP-FE
43	Informes y estadísticas de la Jefatura	Jefatura de la DEP-FE
44	Currícula del personal adscrito a la DEP-FE	Jefatura de la DEP-FE
45	Informes de Actividades de la Planta Académica	Jefatura de la DEP-FE
46	Circulares del Centro de Cómputo	Centro de Cómputo de la DEP-FE
47	Resguardo de Bienes	Delegación Administrativa
48	Expedientes de alumnos	Sección Escolar
49	Evaluaciones de Doctorado (Coloquios)	Sección Escolar
50	Exámenes de Grado	Sección Escolar
51	Proyectos de Investigación (PAPIIT, PAEP, CONACyT, otros)	Profesores e Investigadores de la DEP-FE
52	Registro de usuarios en las salas de cómputo	Centro de Cómputo de la DEP-FE
53	Registro de usuarios en biblioteca	Biblioteca de la DEP-FE
54	Reportes de Ingresos y Egresos	Delegación Administrativa
55	Contratos del personal académico	Delegación Administrativa
56	Datos de usuario	Usuario
57	Envíos por mensajería	Delegación Administrativa

Tabla 4-3. Listado de Activos identificados

Aún cuando el personal se considera como una fuente de amenazas, y que también es considerado como uno de los activos de cualquier organización, no existe un propietario o responsable propiamente dicho ya que lo que respalda su pertenencia a la DEP-FE es un contrato laboral.

4.3.3. Fase 3. Evaluación del riesgo

Una vez identificados los activos, se debe identificar y evaluar las vulnerabilidades y amenazas a las cuales están expuestos para así determinar los riesgos asociados y las medidas que los contrarresten para de determinar la mejor forma de protegerlos.

También se debe enumerar todo tipo de riesgos a los cuales está expuesta la información y cuáles son las consecuencias; enumerar todo tipo de posible pérdida, desde pérdidas directas como tiempo, documentos, equipo, etc., hasta pérdidas indirectas como proyectos cancelados o inconclusos, pérdida de confianza o credibilidad.

Antes de definir lo que es un riesgo retomemos las definiciones expuestas en el capítulo dos:

Vulnerabilidad es un estado en un sistema de cómputo o un grupo de sistemas de información que:

- permite que un atacante ejecute órdenes como si fuera otro usuario.
- permite que un atacante tenga acceso a información restringida.
- permite a un atacante hacerse pasar por otra entidad.
- permite que un atacante genere una negación de servicio.

Amenaza. Una amenaza se define como cualquier factor que impacte de manera negativa al sistema informático o los recursos de la red, el cual puede tener su origen en las personas, la tecnología o por desastre natural.

Riesgo. La Organización Internacional de la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI / TEC TR 13335-1, 1996) como:

> "La posibilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes en un activo o grupo de activos, generándose pérdida o daño"

Realizando una asociación de conceptos, una vulnerabilidad está asociada a una amenaza; una amenaza es cualquier factor que impacte de manera negativa la infraestructura de comunicación o sistemas de información, y el riesgo de ocurrencia de la amenaza está asociado a un impacto dentro de la organización: pérdida o ganancia.

Con estas definiciones en mente y el listado de activos identificados se inició el proceso de ponderación de amenazas y vulnerabilidades, así como la determinación del riesgo asociado a cada uno de los activos de la organización, el cual se muestra en la Tabla 4-4.

Para llegar a esta tabla se definió la posibilidad de ocurrencia como Muy Frecuente o diario, dando un valor de 100; frecuente o mensual, con un valor de 10, y esporádico o anual con un valor de ocurrencia de 1.

Respecto al riesgo se definieron tres valores posibles: alto (A), medio (M) y bajo (B); estos valores se establecieron considerando el impacto que puede tener la sucesión del riesgo en la operación diaria de la DEP-FE.

Infraestructura física

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
1	Edificio			×			Paros estudiantiles o por sindicatos	1	No se tendrá acceso a las áreas de trabajo	B	⇒ Contar con un juego de llaves fuera de las instalaciones
2	Mobiliario			×			Cambio físico del mobiliario y equipo	1	Pérdida del bien	M	⇒ Notificación de cambio de ubicación del bien ⇒ Actualización de resguardo de bienes

Infraestructura de comunicaciones

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
3	Switch	×	×	×	Acceso no autorizado	1			Robo y/o modificación de la información	A	⇒ Seguridad física ⇒ Controles de acceso lógico
		×	×	×	Errores de Configuración	1			Sistemas inestables expuestos a fallas. Pérdida, modificación y divulgación de la información	A	⇒ Configuración especializada ⇒ Capacitación constante
		×	×		Modificación no autorizada de datos	1			Inconsistencia de Datos	A	⇒ Controles de acceso físico y lógico
				×			Apagones o variaciones de voltaje	10	Caída temporal del sistema	A	⇒ UPS con regulador de voltaje ⇒ Líneas de alimentación de corriente independientes
4	Hub			×			Descompostura o mal funcionamiento de los componentes	1	Disminución de la capacidad de respuesta Retraso en la productividad	M	⇒ Stock de reserva
				×			Factores ambientales	1	Daño o destrucción de equipos	B	⇒ Seguridad física ⇒ Ambientación del site
				×			Mantenimiento ineficiente o nulo	1	Mal funcionamiento Disminución de la capacidad Retraso en la productividad	B	⇒ Mantenimiento periódico realizado por especialistas

5	Ruteador	×	×	×	Configuración incorrecta	1			Intrusiones, ataques DoS	B	⇒ Administración especializada
		×	×		Ausencia de pruebas de vulnerabilidad	1			Intrusión, ataques DoS	B	⇒ Ataques programados (hacking ético)
				×			Diseño inadecuado (desde la fabricación)	1	Intrusión, ataques DoS	M	⇒ Conocer las características del equipo (marca y modelo) a través de sitios especializados
				×			Interferencias	1	Errores en líneas de transmisión de datos	B	⇒ Cableado estructurado ⇒ Pruebas de cableado ⇒ Seguridad física
				×			Vida útil	1	Fallas intermitentes Falla parcial de sistemas	B	⇒ Equipamiento actualizado ⇒ Mantenimiento constante
				×			Apagones o variaciones de voltaje	10	Caída temporal del sistema	M	⇒ UPS con regulador de voltaje ⇒ Líneas de alimentación de corriente independientes
6	Conexión de fibra a DGSCA			×	Falla del cableado	1	Fallas en la red de la UNAM	1	Falta del servicio	A	⇒ Monitoreo de funcionamiento de la red UNAM
7	Servidores	×	×	×	Acceso no autorizado	1			Robo y/o modificación de la información	A	⇒ Seguridad física ⇒ Controles de acceso lógico
		×	×	×	Errores de Configuración	1			Sistemas inestables expuestos a fallas. Pérdida, modificación y divulgación de la información	A	⇒ Configuración especializada ⇒ Actualización de versiones, tanto de S.O. como de software de servicios proporcionados
		×	×	×	Modificación no autorizada de privilegios	1			Modificación del sistema	A	⇒ Controles de acceso físico y lógico
				×			Apagones o variaciones de voltaje	10	Caída temporal del sistema	A	⇒ UPS con regulador de voltaje ⇒ Líneas de alimentación de corriente independientes
				×			Descompostura o mal funcionamiento de los componentes	1	Disminución de la capacidad de respuesta Retraso en la productividad	M	⇒ Actualización de componentes ⇒ Cambio de servidor
				×			Factores ambientales	1	Daño o destrucción de equipos	B	⇒ Seguridad física ⇒ Ambientación del site
		×		×			Mantenimiento ineficiente o nulo	1	Disminución de la capacidad de operación Retraso en la productividad	B	⇒ Registros periódicos de la configuración del S.O. ⇒ Mantenimiento realizado por especialistas
8	Equipo de videoconferencia		×	×	Administración inadecuada	1			Falla en el equipo Conexión inexistente	M	⇒ Administración realizada por especialistas ⇒ Capacitación
				×	Acceso no autorizado	1			Robo del equipo	A	⇒ Seguridad física

9	Firewall	×	×	×	Configuración incorrecta	1			Intrusión, ataques DoS	A	⇒ Configuración especializada ⇒ Control de acceso lógico
		×	×	×	Ausencia de pruebas de vulnerabilidad	10			Intrusión, ataques DoS	A	⇒ Ataques programados (hacking ético)
				×			Diseño inadecuado (desde la fabricación)	1	Intrusión, ataques DoS	A	⇒ Conocer las características del equipo (marca y modelo) a través de sitios especializados
		×	×	×			Mantenimiento ineficiente o nulo	100	Mal funcionamiento Disminución de capacidad Retraso en la productividad	A	⇒ Mantenimiento realizado por especialistas

Hardware

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
10	Equipo personal (Monitor, CPU, Teclado, mouse)	×	×	×	Acceso no autorizado	10			Robo y/o modificación de la información	A	⇒ Concienciar a los usuarios ⇒ Seguridad física ⇒ Controles de acceso físico y lógico
		×	×	×	Errores de configuración	10			Sistemas expuestos a fallas y ataques	A	⇒ Generar procedimientos de instalación y configuración de componentes y software ⇒ Configuración especializada
				×	Mantenimiento nulo o incorrecto	10			Funcionamiento incorrecto Pérdida parcial de tiempo y productividad	M	⇒ Bitácora de mantenimiento por equipo ⇒ Mantenimiento preventivo ⇒ Mantenimiento correctivo
		×	×	×	Robo	1			Pérdida de equipo Pérdida de información	A	⇒ Concientizar a los usuarios ⇒ Controles de acceso físico ⇒ Aumento en la vigilancia
		×	×	×			Apagones o variaciones de voltaje	10	Caída temporal del sistema	M	⇒ Uso de UPS con regulador de voltaje ⇒ Líneas de alimentación de corriente independientes o segmentadas
				×			Descompostura o mal funcionamiento de los componentes	10	Disminución de la capacidad de respuesta Pérdida parcial de tiempo y de la productividad	M	⇒ Stock de reserva de componentes más vulnerables
				×			Factores ambientales	1	Degradación de equipos	B	⇒ Instalaciones físicas y uso de aire acondicionado en el área de servidores

				×			Vida útil	1	Depreciación Funcionamiento incorrecto Pérdida de datos	B	⇒ Programas de sustitución de equipo de cómputo de manera periódica
		×	×	×			Virus, malware y spyware	100	Pérdida y/o modificación de información Disminución de la productividad	A	⇒ Capacitación constante ⇒ Respaldos de información ⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
11	LapTop	×	×	×	Acceso no autorizado	10			Robo y/o modificación de la información	A	⇒ Concienciar a los usuarios ⇒ Seguridad física ⇒ Controles de acceso lógico
		×	×	×	Errores de configuración	10			Sistemas inestables expuestos a fallas y ataques	M	⇒ Generar procedimientos de instalación y configuración de componentes y software
				×	Mantenimiento nulo o incorrecto	10			Funcionamiento incorrecto Pérdida parcial de tiempo y productividad	B	⇒ Mantenimiento preventivo ⇒ Mantenimiento correctivo ⇒ Bitácora de mantenimiento por equipo
		×	×	×	Robo	1			Pérdida de equipo Pérdida de información	A	⇒ Concientizar a los usuarios ⇒ Controles de acceso físico ⇒ Vigilancia
				×			Apagones o variaciones de voltaje	10	Caída temporal del sistema	M	⇒ Uso de UPS con regulador de voltaje ⇒ Líneas de alimentación de corriente independientes o segmentadas
				×			Descompostura o mal funcionamiento de los componentes	1	Disminución de la capacidad de respuesta Pérdida parcial de tiempo y de la productividad	B	⇒ Stock de reserva de componentes más vulnerables
				×			Factores ambientales	10	Degradación del equipos	B	⇒ Instalaciones físicas libres de humo y humedad ⇒ Aire acondicionado en el área de servidores
				×			Vida útil	1	Depreciación Funcionamiento incorrecto Pérdida de datos	M	⇒ Programas de sustitución de equipo de cómputo de manera periódica
		×	×	×			Virus, malware y spyware	100	Pérdida y/o modificación de información Disminución de la productividad	A	⇒ Capacitación constante ⇒ Respaldos constantes ⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware

12	Impresora de matriz	×		×	Robo	1			Pérdida de equipo	B	⇒ Controles de acceso físico ⇒ Vigilancia
13	Impresora láser	×		×	Mantenimiento nulo o incorrecto	10			Funcionamiento incorrecto Pérdida parcial de tiempo y productividad	B	⇒ Mantenimiento preventivo ⇒ Mantenimiento correctivo ⇒ Bitácora de mantenimiento por impresora
14	Impresora a color	×		×			Factores Ambientales	100	Degradación del equipo	B	⇒ Condiciones físicas del equipo ⇒ Establecer rutina de apagado de impresoras
15	Impresora doble carta	×		×			Vida útil	1	Depreciación Funcionamiento incorrecto	B	⇒ Mantenimiento preventivo periódico ⇒ Programa de sustitución de impresoras
16	UPS	×	×	×	Deficiencia o ausencia de mantenimiento preventivo	100			Fallas eventuales Retraso en la productividad	B	⇒ Mantenimiento constante y especializado
				×	Robo	1			Pérdida del bien	B	⇒ Controles de acceso físico ⇒ Vigilancia en los cubículos
				×			Apagones prolongados o excesivas variaciones de voltaje	10	Descargas de la bateria del dispositivo	M	⇒ UPS con regulador de voltaje ⇒ Líneas de voltaje segmentadas
				×			Funcionamiento incorrecto	1	Pérdida de información Interrupción de las actividades del personal	B	⇒ Stock de respaldo
				×			Factores ambientales	10	Deterioro del equipo	B	⇒ Stock de respaldo
				×			Vida útil del equipo	10	Fallas intermitentes o parcial de los sistemas	B	⇒ Equipamiento actualizado y con mantenimiento constante
17	Proyector de datos (mini cañón)			×	Deficiencia o ausencia de mantenimiento preventivo	100			Fallas eventuales Retraso en la productividad	B	⇒ Mantenimiento constante y especializado
				×	Robo	1			Pérdida del bien	A	⇒ Controles de acceso físico ⇒ Vigilancia del equipo
				×	Procedimiento inadecuado de apagado	10			Descompostura del equipo	M	⇒ Capacitar al usuario en cuanto al uso del minicañón
				×			Fallas o variaciones de voltaje	10	Degradación del equipo	M	⇒ UPS con regulador de voltaje
				×			Funcionamiento incorrecto	10	Interrupción de las actividades del personal	M	⇒ Stock de sustitución
				×			Factores ambientales	1	Deterioro del equipo	B	⇒ Stock de respaldo
				×			Vida útil del equipo	1	Fallas intermitentes Falla parcial de los sistemas	B	⇒ Equipamiento actualizado y con mantenimiento constante

18	Tarjetas inalámbricas			×			Robo	1	Pérdida del bien	B	⇒ Controles de acceso físico ⇒ Vigilancia
				×			Diseño inadecuado (desde la fabricación)	1	Funcionamiento inadecuado	B	⇒ Conocer las características del equipo (marca y modelo) a través de sitios especializados
19	Teléfono inalámbrico			×	Inadecuada programación o desprogramación	10			Interrupción y retraso en las actividades del personal	M	⇒ Configuración especializada
				×	Uso inadecuado	100			Degradación del bien	B	⇒ Concientizar a los usuarios ⇒ Capacitación.
				×			Robo	1	Ausencia del servicio	B	⇒ Resguardo físico
				×			Vida útil	1	Degradación del equipo	B	⇒ Mantenimiento periódico

Software

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
20	Sistema Operativo		×	×			Desactualización de versiones	10	Huecos de seguridad	M	⇒ Actualización de los "parches" al sistema ⇒ Conocimiento de nuevas vulnerabilidades del S.O.
21	Suite de Escritorio		×				Software sin liencia	10	Funcionamiento incorrecto	A	⇒ Obtener licencias
		×	×	×			Mala o ausencia de compatibilidad de versiones	10	Datos erróneos Inestabilidad del sistema	M	⇒ Revisión de versiones ⇒ Pruebas de migración ⇒ Configuración especializada ⇒ Actualizar service pack
		×	×	×			Virus, malware y spyware	100	Pérdida y/o modificación de información Disminución de la productividad	A	⇒ Capacitación constante ⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
		×	×	×			Falta de restricciones para que el usuario instale programas	1	Comprometer el sistema Incompatibilidad de versiones Huecos de seguridad	A	⇒ Establecer políticas de seguridad para que el usuario no pueda instalar programas
22	Paquetes estadísticos	×	×	×			Ausencia de licencia para uso del producto	10	Inexistencia de soporte técnico Funcionamiento inadecuado	M	⇒ Negociar la adquisición de licencias académicas

		×	×	×			Mala o ausencia de compatibilidad de versiones	10	Datos erróneos Inestabilidad del sistema	M	⇒ Revisión de versiones ⇒ Pruebas de migración ⇒ Configuración especializada
		×	×	×			Desactualización de versiones	10	Huecos de seguridad	A	⇒ Actualizar service pack
		×		×			Errores de configuración	10	Huecos de seguridad	A	⇒ Configuración especializada
		×	×	×			Virus, malware y spyware	1	Pérdida y/o modificación de información Disminución de la productividad	A	⇒ Capacitación constante ⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
23	Manejadores de Bases de Datos	×	×	×	Errores de configuración	1			Huecos de seguridad	A	⇒ Configuración especializada
			×	×			Inadecuado manejo de integridad referencial	10	Inconsistencia de la información	A	⇒ Creación de Base de Datos y esquema de datos ⇒ Gestión de índices ⇒ Implementar una correcta integridad referencial
				×			Servidor con recursos limitados	1	Interrupción del servicio	M	⇒ Gestión de bases de datos alternas
24	Antivirus	×	×	×			Mala configuración	10	Protección inadecuada	A	⇒ Configuración especializada
25	Antispam	×	×	×			Desactualización de la base de datos de virus	10	Pérdida o modificación de la información	A	⇒ Actualización de la base de virus detectables
26	Herramientas de Desarrollo	×	×	×			Ausencia de licencias	1	Problemas legales a menos que sea de distribución libre	A	⇒ Adquisición de licencias ⇒ Actualización de versiones
		×	×	×			Conocimientos insuficientes	10	Escasa confiabilidad de los datos Sistema susceptible a errores humanos	A	⇒ Capacitación constante al desarrollador ⇒ Acceso a la documentación
		×	×	×			Errores de configuración	10	Sistemas inestables y expuestos a ataques	A	⇒ Configuración especializada

Servicios

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
27	Servidor de correo	×	×	×			Saturación del servidor	1	Interrupción del Servicio	A	⇒ Establecer cuotas bajas de espacio en el servidor

		×		×			Desactualización de versiones	1	Huecos de seguridad	A	⇒ Actualizar versiones del servidor de correos
		×	×	×			Virus, malware y spyware	10	Pérdida y/o modificación de información	A	⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispam
28	Servidor de la Página web de la DEP-FE	×	×	×	Errores de configuración	10			Huecos de seguridad	A	⇒ Configuración especializada
				×			Falla del switch	10	Ausencia del servicio	M	⇒ Configuración especializada ⇒ Alimentación eléctrica estable y constante
		×	×	×			Inexistencia de firewall	100	Accesos no deseados	A	⇒ Implementar firewall ⇒ Configuración especializada
				×			Falla en la red	10	Ausencia del servicio Retraso en la operación	A	⇒ Monitoreo constante
		×	×	×			Virus, malware y spyware	1	Pérdida y/o modificación de información	A	⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
		×	×	×			Vida útil	10	Interrupción en las actividades cotidianas	A	⇒ Concientizar a las autoridades de la importancia de contar con un servidor en forma
29	Servidor de las Bases de Datos de la DEP-FE	×	×	×			Inexistencia de firewall	100	Accesos no deseados	A	⇒ Implementar firewall ⇒ Configuración especializada
		×	×	×			Ausencia de respaldos	10	Imposibilidad de recuperar la operación	A	⇒ Gestión de respaldos de datos ⇒ Gestión de almacenamiento de respaldos
		×	×	×			Accesos no autorizados	10	Modificaciones no autorizadas	A	⇒ Gestión de perfiles ⇒ Gestión de usuarios ⇒ Gestión de registro de transacciones ⇒ Implementación de claves de acceso
			×	×			Falla del switch	10	Errores de datos Interrupción del servicio	A	⇒ Revisiones constantes de versiones ⇒ Configuración especializada ⇒ Alimentación eléctrica estable y constante ⇒ Uso de UPS
		×	×	×			Virus, malware y spyware	1	Pérdida y/o modificación de información	A	⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
30	Servidor de la plataforma educativa	×	×	×	Error de configuración	1			Pérdida de información, cursos o material en línea	A	⇒ Configuración especializada ⇒ Actualización constante

	Moodle		×	×			Falla de la Red	10	Interrupción de la operación	A	⇒ Monitoreo constante
		×	×	×			Ausencia de firewall	100	Accesos no deseados	A	⇒ Implementar firewall ⇒ Configuración especializada
			×	×			Falla del switch	10	Errores de datos Interrupción del servicio	A	⇒ Revisiones constantes de versiones ⇒ Configuración especializada ⇒ Alimentación eléctrica estable y constante ⇒ Uso de UPS
		×	×	×			Virus, malware y spyware	1	Pérdida y/o modificación de información	A	⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
31	Servidor de la Biblioteca	×					Acceso no autorizado	1	Pérdida y/o robo de información	A	⇒ Monitoreo constante
				×			Falla en la red universitaria	1	Ausencia de servicio	A	⇒ Monitoreo constante
32	Fotocopiado	×	×	×			Copias no autorizadas	10	Robo de información	A	⇒ Implementar un control más estricto de fotocopiado
							Vida útil del equipo	1	Interrupción del servicio	A	⇒ Contar con área de fotocopiado alterna

Sistemas de Información

	Activos	**Servicios de Funcionalidad**			**Vulnerabilidad**	**Frecuencia**	**Amenaza**	**Frecuencia**	**Riesgo**	**Ponderación**	**Medidas**
		C	**I**	**D**							
33	Sistema de Información de la Jefatura de la DEP-FE	×	×	×	Visualización del Full-path	10			Robo, modificación y/o divulgación de la información	A	⇒ Actualización de ligas ⇒ Manejo de sesiones de usuario
		×	×	×	Malware y spyware	100			Pérdida, modificación, divulgación y/o pérdida de datos. Disminución de la productividad.	A	⇒ Antivirus, Antispyware, firewall personal ⇒ Antivirus actualizado
34	Sistema de Información de la Planta	×	×	×	Virus	100			Modificación, pérdida y/o divulgación de datos. Disminución de la productividad.	A	⇒ Antivirus, Antispyware, firewall personal ⇒ Capacitación constante
		×	×	×			Levantamiento de	10	Resolución inadecuada	A	⇒ Conocimiento de las reglas del negocio

	Académica de la DEP-FE						requerimientos de usuario deficiente		de problemas		⇒ Definir procesos de operación correctos ⇒ Definir alcance del sistema
35	Sistema de alumnos de Doctorado en Economía	×	×	×			Programación cerrada (no susceptible a cambios)	10	Sistemas inestables sin opción a cambios de programación	A	⇒ Análisis y diseño de sistemas ⇒ Parametrización ⇒ Programación Orienta a Objetos
		×	×	×			Pruebas deficientes	10	Baja confiabilidad del sistema	A	⇒ Ampliación de pruebas ⇒ Análisis y diseño estructurado ⇒ Análisis y diseño orientado a objetos
36	Sistema de alumnos de Maestría en Economía	×	×	×			Ausencia de mecanismos de encriptamiento	10	Captura, modificación y/o divulgación de la información	A	⇒ Implementación de mecanismos de encriptamiento
		×	×	×			Errores en las funciones de encriptamiento	10	Divulgación de información	A	⇒ Utilización de protocolos de seguridad durante la transmisión (SSH) ⇒ Evitar en lo posible los servicios del FTP y Telnet ⇒ Pruebas de transferencia de datos
37	Sistema del Programa Único de Especialización En Economía	×	×	×			Deficiente integridad de datos	1	Inconsistencia de la información	A	⇒ Controles de validación de datos ⇒ Implementar integridad referencial en la(s) Bases de datos
		×	×	×			Perdida de confidencialidad	1	Divulgación de la información	A	⇒ Controles de acceso lógico y físico en todos los datos ⇒ Seguimiento de actividades de los usuarios dentro de la base de datos
38	Sistema de la Coordinación del Programa de Posgrado en Economía		×	×			Ausencia de documentación	10	Retraso en el mantenimiento y actualizaciones	A	⇒ Generar documentación de sistemas ⇒ Actualización constante de la documentación
				×			Medios de datos no disponibles	1	Disminución de confiabilidad Retraso en las actividades laborales	A	⇒ Respaldos periódicos ⇒ Actualizaciones de versiones del DBMS
		×	×	×			Ausencia de respaldos	10	Retraso en las actividades cotidianas	A	⇒ Respaldos periódicos
39	Sistema de Inventarios	×	×	×			Sabotaje	1	Pérdida o robo de la información	A	⇒ Utilización de protocolos de seguridad durante la transmisión (SSH)
		×	×	×			Spoofing y sniffing	1	Divulgación y/o robo de la información	A	⇒ Utilización de switches
40	Código Fuente	×	×	×	El código contiene backdoors	1			Divulgación de la información	A	⇒ Auditorias a la programación
		×	×	×	No se cuenta con programas fuente	1			Sistema limitado a futuro ya que no puede ser adecuado a nuevas	A	⇒ Administración de versiones de desarrollo ⇒ Respaldos periódicos de los programas fuente

									necesidades		
		×		×	Documentación inexistente o no actualizada	1			El programa puede realizar funciones de las cuales no se tiene conocimiento	A	⇒ Generar documentación técnica ⇒ Auditorias a la programación
		×	×	×	Ausencia de resguardados	10			Pérdida de procedimientos Retraso en los desarrollos	A	⇒ Resguardos periódicos del código fuente
41	Bases de datos	×	×	×	SQL Injection	10			Modificación, divulgación y/o pérdida de datos	A	⇒ Configuración del servidor de BD ⇒ Análisis de sentencias SQL antes de su ejecución
		×	×	×			Base de datos compleja	10	Programación compleja de interfase	A	⇒ Se apoya en el DBMS para mantener la integridad de la información a través del diseño de la BD
		×	×	×					Desarrollo de sistemas complejo	A	⇒ Desarrollo de aplicaciones en capas ⇒ Documentación de los desarrollo
		×	×	×					Errores de validación	A	⇒ Validar datos de entrada
		×	×	×			Copia no autorizada de datos	10	Divulgación de la información	A	⇒ Configuración del servidor ⇒ Cancelar opciones de copiado
		×	×	×			Inconsistencia de los datos	10	Retraso en las actividades	A	⇒ Auditorias periódicas a la base de datos
		×	×	×			Falla de copias de seguridad	10	Pérdidas de respaldos	A	⇒ Respaldos periódicos ⇒ Verificación de las restauraciones
		×	×	×			Robo	10	Divulgación de la información	A	⇒ Controles físicos de acceso a los servidores y datos de misión crítica
		×	×	×			Sabotaje	10	Modificación y/o pérdida de la información	A	⇒ Controles físicos de acceso a los servidores y datos de misión crítica ⇒ Registro de accesos a la BD

Documentación

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Frecuencia	Amenaza	Frecuencia	Riesgo	Ponderación	Medidas
		C	I	D							
42	Oficios de la Jefatura	×					Pérdida de documento	10	Divulgación de la información	A	⇒ Contar con personal de confianza
				×			Retraso en la entrega	10	Pérdida de tiempo	A	⇒ Concienciar a los involucrados ⇒ Calendarizar entregas

43	Informes y estadísticas de la Jefatura	×		×			Robo	10	Pérdida, modificación y/o divulgación de la información	M	⇒ Resguardo físico de la información
44	Curricula del personal adscrito a la DEP-FE	×		×			Robo	1	Pérdida, modificación y/o divulgación de la información	M	⇒ Archivo físico controlado ⇒ Resguardo de documentación
45	Informes de Actividades de la Planta Académica	×		×			Robo Ausencia de informes	10	Pérdida, modificación y/o divulgación de la información Retraso en las operaciones	M	⇒ Concientizar a los profesores de la entrega de informes
46	Circulares del Centro de Cómputo	×		×			Ignorar las circulares	10	Retraso en la productividad Sobrecarga de actividades	M	⇒ Retraso en la colaboración de usuarios y personal ⇒ Concientizar a los usuarios de los servicios
47	Resguardo de Bienes	×	×	×			Robo	1	Pérdida del bien	A	⇒ Cámaras de vigilancia ⇒ Revisión de bultos o mobiliario a la salida del edificio
48	Expedientes de alumnos	×	×	×			Divulgación y/o robo de información	1	Pérdida de información	A	⇒ Sistema de Archivo controlado
49	Evaluaciones de Doctorado (Coloquios)	×	×	×			Divulgación y/o robo de información	1	Reprogramación de evaluaciones Retraso en la productividad	A	⇒ Crear zona especial para atención de alumnos ⇒ Registro constante y respaldo de las modificaciones y/o confirmación de las evaluaciones
50	Exámenes de Grado	×	×	×			Divulgación y/o robo de información	1	Reprogramación de evaluaciones Retraso en la productividad	A	⇒ Crear zona especial para atención de alumnos ⇒ Registro constante y respaldo de las modificaciones y/o confirmación de las evaluaciones
51	Proyectos de Investigación (PAPIIT, PAEP, CONACyT, otros)	×		×	Impresoras y directorios compartidos	10	Divulgación y/o robo de información	1		A	⇒ Control de acceso al área de trabajo ⇒ Evitar el uso de impresoras compartidas ⇒ No olvidar impresiones realizadas
				×			Falta de espacio de almacenamiento	10	Retraso en la productividad	M	⇒ Uso de medios externos de almacenamiento: USB, DVD, CD
		×		×			Copias no autorizadas	1	Divulgación o mal uso de la información	A	⇒ Controles físicos de acceso
		×		×			Robo	1	Pérdida de información Retraso en la productividad	A	⇒ Controles físicos de acceso
		×		×			Sabotaje	1	Pérdida o robo de la información	A	⇒ Respaldos periódicos ⇒ Control de versiones
		×	×	×			Virus, malware y	100	Pérdida o modificación	A	⇒ Capacitación constante

							spyware		de la información Retraso en la productividad		⇒ Antivirus actualizado ⇒ Firewall correctamente configurado ⇒ Antispyware
52	Registro de usuarios en las salas de cómputo	×		×			Ausencia de registro	10	Pérdida de información	A	⇒ Bitácoras de ingreso ⇒ Resguardo de bitácoras ⇒ Registro automatizado de usuarios
53	Registro de usuarios en biblioteca	×		×			Ausencia de registro	100	Ausencia o pérdida de información Ausencia de estadísticas de uso	A	⇒ Registros de acceso ⇒ Respaldos de registros de acceso ⇒ Respaldos de la base de consultas
54	Reportes de ingresos y egresos	×	×	×			Robo	1	Divulgación de información Pérdida de documentos	A	⇒ Resguardo correcto de la información
55	Contratos del personal académico	×	×	×			Alteración del contrato Pérdida del documento Datos incorrectos	10	Pérdida de tiempo Problemas en ejercicios presupuestales Retraso en nómina	A	⇒ Capacitación al personal del área ⇒ Seguimiento de nombramientos
56	Datos de usuario	×	×	×	Accesos no autorizados	10			Modificación, pérdida y/o divulgación de la información	A	⇒ Restringir acceso físico ⇒ Implementar criptografía
		×		×	Capacitación y/o conocimientos insuficientes	10			Sistemas susceptibles a errores humanos Descompostura del equipo de cómputo	A	⇒ Capacitación ⇒ Políticas de seguridad en los equipos de escritorio
		×	×	×	Virus, malware y spyware	100			Pérdida, modificación y/o divulgación de la información Disminución de la productividad	A	⇒ Antivirus actualizados ⇒ Antispyware con configuración especializada ⇒ Firewall personales
		×	×	×			Deficientes controles de acceso	10	Modificación, pérdida y/o divulgación de la información	A	⇒ Contraseñas de acceso ⇒ Protectores de pantalla con contraseñas
		×	×	×			Robo de información	10	Pérdida de información Retraso y descontento	A	⇒ Respaldos constantes ⇒ Controles físicos de acceso a las áreas de trabajo
57	Envíos por mensajería	×	×	×			Pérdida del envío	1	Divulgación de la información Retraso en trámites	A	⇒ Seguimiento a los paquetes ⇒ Confirmar entrega de envío

Usuarios

	Activo	Servicios de Funcionalidad			Vulnerabilidad	Fre-cuencia	Amenaza	Fre-cuencia	Riesgo	Pon dera ción	Medidas
		C	I	D							
58	Alumnos	×					Robo de documentación	10	Pérdida de información	A	⇒ Escritorios libres de documentación ⇒ Área específica para atender a alumnos
		×	×	×			Modificación de información	1	Degradación de la confiabilidad de la información	A	⇒ Crear área exclusiva de atención a alumnos ⇒ Concienciar a los alumnos de responsabilzarse de sus trámites escolares
59	Profesores invitados	×					Falta de espacio	1	Pérdida de información	B	⇒ Designar un área específica para personas invitadas
		×					Instalación de paquetes de cómputo	100	Generar huecos de seguridad Incompatibilidad de versiones	B	⇒ Proporcionar equipo de cómputo con políticas de seguridad
60	Personas externas a la institución	×		×			Ausencia de registro de ingreso	10	Robo o modificación de bienes	M	⇒ Cámara de vigilancia
		×					Ausencia de registros de ingreso	10	Modificación, pérdida y/o divulgación de información	M	⇒ Implementación de registros de visitas
		×	×	×			Robo de documentación	10	Pérdida de información	A	⇒ Escritorios libres de documentación ⇒ Área específica para atender a alumnos

Tabla 4-4. Evaluación del riesgo

4.3.4. Fase 4. Gestionar el Riesgo

En esta etapa se determina la postura que tomará la entidad académica con respecto al riesgo detectado mediante la selección e implantación de un buen control que permita su reducción a un nivel aceptable.

a) Selección de controles

La selección de controles a implementar debe ser tomada basados en el binomio activo-impacto en la organización.

El estándar ISO 17799 en [12] indica que para el tratamiento de problemas de seguridad se puede adoptar una de las siguientes posturas:

- *Evitar* el riesgo
- *Aceptar* objetivamente el riesgo partiendo del supuesto que satisfacen la política de la organización y se está preparado para asumir las consecuencias del hecho
- *Reducir* el riesgo mediante la aplicación de controles apropiados
- *Transferir* el riesgo a un tercero mediante la contratación de un seguro o la contratación de terceros (outsourcing)

Las acciones antes mencionadas pueden adoptarse en cualquier momento, pero se debe tener muy presente que ignorar un riesgo nunca es una solución conveniente.

Los riesgos detectados fueron analizados en tres momentos: antes (prevención), durante (detección) y después de un ataque (corrección); de igual manera el control a implementar debe estar presente en cada uno de estos momentos abarcando aspectos físicos, técnicos y organizacionales a cubrir.

i. Prevención

Consiste en mecanismos que incrementan el nivel de seguridad de un sistema durante su funcionamiento normal de tal manera que se evite el fallo o, si es el caso, se aminoren las consecuencias que de ello se puedan derivar. La Tabla 4-5 presenta ejemplos de este tipo.

Prevención Física	Prevención Técnica	Prevención Organizacional
Ubicación del área de servidores	Líneas de la potencia eléctrica	Selección de personal
Resguardo de Servidores	Buenas práctica de respaldos o backups	Control de accesos
Resguardo de instalaciones físicas	Claves de acceso robustas para equipos y aplicaciones	Límites de ámbito de acción del personal
Resguardo de documentos	Uso de métodos criptográficos	Cursos de actualización
Sistemas contra incendios	Bitácora de eventos críticos	
	Actualización de parches de	

	seguridad de los S.O.	
	Subneteo correcto	
	Firewalls personales y corporativos	

Tabla 4-5. Prevención de Riesgos

ii. Detección

Mecanismos orientados a evidenciar violaciones o intentos de violación a la seguridad. Generalmente se componen por programas de auditoría. La Tabla 4-6 nos presenta algunos mecanismos orientados a la detección.

Detección Física	Detección Técnica	Detección Organizativa
Monitor de vigilancia	Control de acceso lógico	Auditorias periódicas
Detector de metales	Sesión de autenticación	
Detector de movimiento	Control de integridad de archivos	
Revisión de maletas, paquetes, etc.		

Tabla 4-6. Detección de riesgos

iii. Corrección

Mecanismos que se implementan una vez realizada la violación al sistema o identificada la vulnerabilidad a fin de reestablecer el funcionamiento normal con la seguridad e integridad de los datos validada. La Tabla 4-7 muestra algunas sugerencias a este respecto.

En esta etapa también se realiza la confirmación y aceptación de la mejora o corrección realizada.

Correctiva Física	Correctiva Técnica	Correctiva Organizacional
Respaldo de alimentación eléctrica	Corrección de defectos	Respaldos programados
	Confirmación y aceptación de la evaluación	Plan de incidentes (sanciones)
	Certificación	

Tabla 4-7. Corrección de Riesgos

4.3.5. Fase 5. Seleccionar objetos de control y controles a implementar

Un control se define como el conjunto de acciones, documentos, procedimientos, técnicas y medidas a adoptar, las cuales tienen como objetivo reducir los riesgos de seguridad, en este caso dentro de la DEP-FE.

En esta etapa también se debe establecer la *calidad de la información*, es decir se debe establecer cuándo o para quién la información debe ser confidencial, cuándo debe verificarse su integridad y cuándo la autenticidad, tanto de la información como de los usuarios.

Una vez planteado el valor de la información, es decir qué tanto se pierde si le ocurre algo a la información o qué tanto se gana si está protegida, se deben establecer las medidas para que cumpliendo con la política de seguridad las perdidas sean las menores posibles y que esto se transforme en ganancias, ya sean materiales o de imagen.

A continuación se listan los objetos de control seleccionados para las distintas fuentes de amenaza o vulnerabilidad detectadas.

4.3.5.1. Seguridad Física

La seguridad física se dividió en varios aspectos, todos ellos enfocados a reducir el riesgo de pérdida de información o interrupción de procesos.

a) Acceso al edificio, motivado por la asistencia a clases, conferencias o eventos culturales, principalmente.

Se propone un control de visitantes hacia las áreas académicas y administrativas. Dicho control deberá indicar los elementos mostrados en la tabla 4-8.

FECHA	NOMBRE	PROCEDENCIA	PERSONA QUE VISITA	MOTIVO	HORA DE ENTRADA	HORA DE SALIDA

Tabla 4-8. Propuesta de registro de accesos

Este puede ser un control sencillo, pero que nos dará idea del tipo de personas, además de los alumnos, que hacen uso de las instalaciones de la DEP-FE.

b) Control de acceso y salida de paquetes. Todo paquete deberá ser revisado por el personal de vigilancia al ser ingresado o retirado del edificio, así como indicar el área origen o destino.

c) Acceso a Cubículos. Para el ingreso a los cubículos de profesores se propone la asignación de personal de vigilancia o de apoyo secretarial al inicio del área, a fin de que se permita o niegue el acceso al visitante; este acceso estará condicionado a la presencia del académico y se utilizará un formato similar al utilizado para el acceso al edificio.

d) Suministro eléctrico. Se debe contar con una línea dedicada y debe ser monitoreada de manera constante. Como respaldo a la línea, se ha dotado a cada equipo de cómputo con un UPS a fin de proporcionar energía suficiente para que el usuario almacene su información y apague el equipo sin problemas en caso de suscitarse el problema.

e) Cableado estructurado. Se debe documentar el tendido de los cables y conexiones de red mediante planos y esquemas, actualizándolos cada que se modifique. De igual manera, se debe mantener oculto este tendido.

f) Seguridad de los equipos de escritorio. La mayor parte de las actividades se realizan utilizando como herramienta los equipos de escritorio, por lo que debe asegurarse las condiciones físicas de operación de este tipo de equipo. De igual manera se deben proteger los componentes para que no sean sustraídos de las respectivas áreas.

g) Acceso al área de servidores. Esta área es muy sensible a la información, por lo que toda persona que ingrese a esta área deberá registrarse. Debido a su importancia, sólo el responsable de los servidores deberá permanecer en dicha área.

h) Seguridad en los Laboratorios y Salas de Cómputo. Estas áreas, al ser áreas de servicio al público deben estar especialmente vigiladas y controladas, por lo que personal del Centro de Cómputo estará a cargo de esta tarea, implementando registros de acceso, verificación de dispositivos de almacenamiento externo y permanencia física de los equipos de cómputo y sus componentes.

i) Seguridad en los Escritorios. Los escritorios son áreas que siempre tienen diferente tipo de información, por lo que debe ponerse especial atención en cuanto a la permanencia de los documentos soporte y evitar en lo posible dejar a la vista información privada o de uso interno.

j) Seguridad en equipos de Fotocopiado y Fax. Estas áreas, al proporcionar servicios que son utilizados por casi todo el personal, deben estar controladas en cuanto a los documentos que se reciben y entregan a los usuarios.

k) Registro de Inventario. Todo equipo de cómputo que sea asignado a la DEP-FE deberá ser registrado de manera inmediata y quedar bajo resguardo de un responsable, ya se el encargado del Centro de Cómputo o un usuario previamente definido

l) Mantenimiento de los equipos de cómputo. Ésta es una de las formas más económicas de prevenir la pérdida de información, ya que el mantenerlo en óptimas condiciones alarga su vida útil.

4.3.5.2. Seguridad Lógica

Los controles a implementar deben hacer hincapié en la necesidad de administrar y controlar todo lo que sucede en la red a fin de evitar amenazas, así como configurar los equipos ad-hoc a las necesidades de la DEP-FE, ya que las configuraciones estándar o de fábrica no siempre protegen de manera correcta para una infraestructura específica.

Para realizar este control se presenta un nuevo diseño de la red de comunicaciones de la DEP-FE a fin de mejorar tiempos de respuesta, rendimiento del ancho de banda y protección de los equipos personales; también se propone la creación de un cuarto de red, con los equipos de Telecomunicaciones necesarios para dar soporte a las necesidades propias de la DEP-FE.

a) Segmentación de la Red

Actualmente la red de comunicaciones de la Facultad de Economía tiene el mayor tráfico en las áreas académicas y administrativas correspondientes a la División de Estudios Profesionales, tal como lo muestra la Figura 4-3, por lo que se propone una segmentación de la red donde quede aislado el tráfico correspondiente a las actividades propias de la DEP-FE (Figura 4-4).

Esta segmentación ayudará en el aislamiento del tráfico, disminución de ataques externos, optimizar el ancho de banda y monitoreo del tráfico perteneciente únicamente a las áreas propias de cada división, y específicamente las del Posgrado

b) Instalación y configuración de firewalls y proxies

Otra implementación que debe realizarse es la de un firewall que permita filtrar el tráfico no deseado a la red interna del posgrado.

La postura inicial debe ser de negación preestablecida, es decir, negando todos los protocolos y servicios para posteriormente habilitar sólo los necesarios para la operación de la DEP-FE.

El uso y configuración de Firewalls personales en los equipos de misión crítica también se debe implementar por la naturaleza y clasificación de la información en ellos contenida.

La Figura 4-3 nos muestra el diagrama de red propuesto.

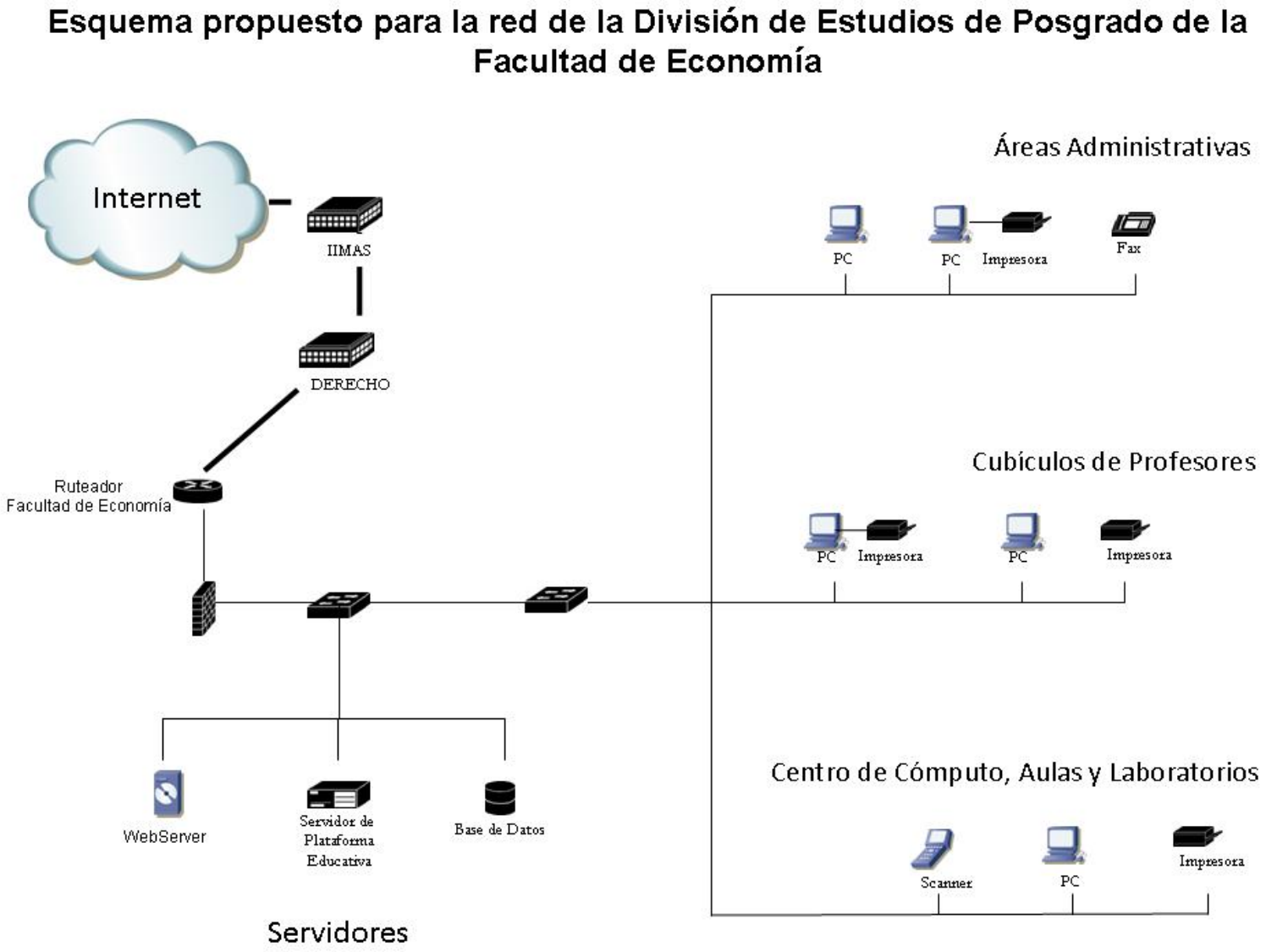

Figura 4-3. Propuesta de Segmentación de la red de la DEP-FE

c) Administración de la red

La administración de la red consiste en un conjunto de operaciones que se llevan a cabo para lograr un óptimo desempeño de una o varias redes de datos.

La operación en la administración de la red involucra funciones tales como mantenimiento y configuración de dispositivos, monitoreo y atención a falla. Otra actividad a realizar es la planeación, ya que mediante ella se obtienen estadísticas de desempeño, análisis y diseño de la infraestructura, así como crecimiento y servicios proporcionados.

La buena o mala administración que se realice de la red tendrá como resultado una buena o deficiente protección de los recursos y de la información.

d) Antivirus

Los equipos de cómputo de la DEP-FE se configuran de tal manera que se incluya un antivirus como parte de las aplicaciones básicas y de uso cotidiano. Para su actualización, se ha destinado un equipo de cómputo específico para que los usuarios se conecten y actualicen la base de datos de virus detectables en su equipo personal y realicen por sí mismos el escaneo y limpieza de su equipo. Esta base de datos es actualizada cotidianamente por personal del Centro de Cómputo.

También se ha implementado la realización semestral de campañas antivirus, siempre antes del inicio del semestre lectivo, para que los usuarios cuenten con equipo libre de virus y actualizado en cuanto a versiones suites de escritorio.

e) Dispositivos de los equipos de escritorio

Si bien los equipos de escritorio se encuentran dotados de lectoras de discos flexibles y puertos USB, éstos son una fuente de amenaza a la información, es por ello que se debe proteger los equipos y deshabilitar aquellos dispositivos que no requieran ser utilizados.

f) Autenticación

La autenticación en los sistemas de información se la DEP-FE se ha vuelto obligatorio.

Aún cuando se designe un login y password para los usuarios en cada sistema, también se debe instruirlos para que el password no sea fácilmente adivinado o robado, con los cual se pone en riesgo la información registrada.

g) Password

Es obligatorio para todos los usuarios el uso de passwords en los sistemas de información de la DEP-FE.

Mediante estos mecanismos se está protegiendo la identidad del usuario a la vez que se registran las actividades realizadas dentro de la base de datos, por lo que es de suma importancia contar con ellos.

Estos password deben estar conformados de tal manera que realmente representen un mecanismo de seguridad, por lo que en su creación y operación deben seguirse las políticas definidas para su conformación.

h) Sesiones de usuario

Las sesiones de usuario son un mecanismo de control mediante el cual se permite el acceso o negación del servicio a un usuario.

Estas sesiones son validas en cada página web, por lo que cuando ésta es accesada realiza la validación, permitiendo o no su desplegado en el lado del cliente. Esta proceso se realiza a fin de que cada acceso sea solicitado y respondido a un usuario previamente validado en el sistema.

i) Administración de controles de acceso

Los controles de acceso a la información se dividen en:

- Acceso de sólo lectura
- Acceso de escritura
- Acceso de modificación

estos accesos son asignados en base a una matriz de roles de usuario / módulos de los sistemas desarrollados, misma que es definida por los directivos en base a las actividades y ámbito de acción de los usuarios.

El despliegue de la información se realiza de manera específica para el usuario en cuestión y en concordancia con los permisos que tengan asociados, tal como lo muestra la Tabla 4-9 de acuerdo con sus funciones, responsabilidades y actividades de cada uno.

Grupo de Trabajo	Usuario	Módulo	Lectura	Escritura	Modificación
Jefatura	Jefe de División y Secretario Académico	Planta Docente	x	x	x
		Carga Académica en la DEP-FE	x	x	x
		Premios y distinciones	x		
		Dirección de Tesis	x		
		Difusión Académica Profesores	x		
		Eventos organizados DEP-FE	x	x	x
Sección Escolar	Maestría	Ingreso	x	x	x
		Asignación de Tutor	x	x	x
		Asignación de Campo de Conocimiento	x	x	x
		Historia Académica	x	x	x
		Dirección de Tesis	x	x	x
		Examen de Grado	x	x	x
		Seguimiento	x	x	x
	Doctorado	Ingreso	x	x	x
		Asignación de Tutor	x	x	x
		Asignación de Campo de Conocimiento	x	x	x
		Actividades Académicas	x	x	x
		Dirección de Tesis	x	x	x
		Coloquio de Doctorado	x	x	x
		Candidatura a Doctor	x	x	x
		Examen de Grado	x	x	x
		Seguimiento	x	x	x
Profesores	Profesor	Datos Personales	x	x	x
		Grados académicos	x	x	x
		Carga Académica	x	x	x
		Dirección de Tesis	x	x	x
		Difusión Académica Profesores	x	x	x
		Publicaciones	x	x	x
Apoyo Secretarial	Secretaria	Difusión Académica Profesores	x	x	x
		Eventos organizados DEP-FE	x	x	x
Delegación Administrativa	Secretaria	Datos Personales Docente	x	x	
		Nombramientos Académicos	x	x	x
		Licencias y sabáticos	x	x	x
Gestión	Administrador	Catálogos	x	x	x
		Administración de usuarios	x	x	x
Público en general		Curricula de tutores y profesores	x		
		Campos de Conocimiento	x		

Tabla 4-9. Resumen de permisos de usuario

4.3.5.3. Seguridad en los Sistemas de Información

Aún cuando se haya instalado un firewall, se haya segmentado la red, o se hayan configurado los servidores web para reducir las vulnerabilidades y amenazas, esto puede resultar aún insuficiente ya que estos dispositivos no realizan un análisis del código HTML, lo cual implica que se puede dejar pasar un porcentaje significativo de ataques web; es por ello que se hace necesaria la protección de los sistemas de información utilizados y/o desarrollados por personal de la DEP-FE.

En cada etapa de análisis, diseño e implementación de sistemas de información se debe realizar una valuación del riesgo. A continuación se presenta la forma en que fueron desarrolladas las aplicaciones web de la DEP-FE, lo que a su vez generó la creación de políticas de seguridad indicadas en el apartado de Seguridad de los Sistemas de Información de dicha política.

a) Análisis de Sistemas de Información

Debido al desarrollo tecnológico y a la capacitación que esto implica, la DEP-FE no contaba con sistemas de información hasta el año de 2005, cuando se inició un esfuerzo por automatizar las actividades realizadas por esta División.

Inicialmente se llevó a cabo un levantamiento de requerimientos, mismos que fueron enriqueciéndose conforme se avanzó en el desarrollo de los sistemas.

Como las actividades se encontraban centradas en las personas y no en las funciones, esta etapa consumió más tiempo del estimado debido a que el personal no tenía conocimiento completo del área y, como consecuencia, de las actividades que en ella se realizan.

De esta etapa se derivó la identificación de usuarios y roles, así como su ámbito de acción al generar el modelo conceptual de los sistemas desarrollados.

b) Desarrollo de Sistemas de Información

El desarrollo de los sistemas se realizó en etapas ponderando las necesidades de las diversas áreas de trabajo.

En cada etapa se fueron refinando los requerimientos, a la vez que surgían nuevas necesidades del usuario; de igual manera, cuestiones de seguridad fueron implementadas. Por ejemplo, en un inicio se tenía una definición de usuarios y su ámbito de acción (profesores, jefatura, escolares-maestría y administrador del sistema), donde el enfoque empleado fue que cada usuario sólo tenía acceso a su información. Conforme se fue avanzando en el desarrollo y los usuarios fueron conociendo las opciones de los sistemas, consideraron que también necesitan utilizar la *opción x* o *y*, por lo que los requerimientos fueron cambiando, los accesos se fueron registrando y las aplicaciones crecieron adecuándose para ser compartidas por diversas áreas. Esto trajo a su vez el problema de confidencialidad e integridad, por lo que se hizo necesario modificar el alcance de los sistemas e implementar controles, registros de accesos y encriptar datos confidenciales.

Mediante la estrategia de entrega por etapas se pudo cuantificar el avance global de los desarrollos, así como validar la consistencia con los requerimientos especificados en cada etapa, ya que éstos fueron cambiando conforme se fue avanzando.

De igual manera, en cada etapa se realizó una verificación del funcionamiento del sistema a fin de disminuir correcciones en etapas futuras, llevando al mismo tiempo un control de versiones para poder "regresar" a la versión anterior, si fuese necesario.

Con respecto a la codificación, se establecieron estándares de identificación para tipos de datos (numérico, carácter, lógico, …), procesos a realizar (captura, modificación, consulta, …); también se estableció una estructura de directorios para las diversas opciones de los sistemas, a fin de controlar y mantener el orden lógico de las operaciones y procesos a realizar.

c) Documentación de los desarrollos

Inicialmente no existía documentación alguna, sin embargo ésta se fue generando a la par del avance de los sistemas, por lo que a la fecha se tienen documentados los procesos de las aplicaciones.

La importancia de la documentación radica en la referencia que se hace hacia ella, ya que para cualquier modificación a los sistemas se requiere la revisión del impacto en el resto de los sistemas con los que colabora.

De igual manera es necesaria para cuando se requiera implementar un DRP.

d) Mantenimiento de los Sistemas de Información

El mantenimiento a los Sistemas de Información es una actividad que se realiza de manera permanente ya que las necesidades de los usuarios se modifican o incrementan, por lo que cualquier cambio o nuevo proceso a incorporar debe ser documentado a lo largo de todo el proceso de desarrollo, pruebas y liberación de cambios.

e) Diseño de interfaz

El diseño de la interfaz con el usuario fue uno de los aspectos que más trabajo requirió al inicio del proyecto, ya que a partir de ahí se inició con la programación de todas las páginas de los sistemas.

Esta interfaz se implementó mediante una combinación de herramientas web que permiten el manejo de contenidos, apariencia y comportamiento de las páginas a través de las opciones implementadas; esto proporciona una visión institucional a lo largo de cada sistema y permite una navegación sencilla indicando en todo momento el sistema y opción que se está utilizando.

En la Tabla 4-10 se enumeran las herramientas utilizadas así como los elementos afectados.

Herramienta Web	Aplicable a	Ejemplos
HTML	Estructura	Párrafos, encabezados, listas, tablas
	Contenido	Texto, imágenes, enlaces
CSS	Apariencia	Colores, tipografía, alineación, fondos, tamaños
JavaScript	Comportamiento	Efectos, validaciones, automatización

Tabla 4-10. Herramientas web utilizadas

Para realizar el diseño uniforme e institucional se generó una hoja de estilo (CSS) que es utilizada en todos los documentos HTML de los sistemas. El uso de hojas de estilo permiten ahorrar tiempo y trabajo tanto en la administración como en la actualización del diseño, de tal manera que cuando se desea cambiar el aspecto de todas las páginas o de los elementos en ellas contenidos sólo será necesario modificar el archivo de la hoja de estilo (archivo *.css) y no la llamada a éste que se realiza en cada archivo HTML.

f) Interactividad de las aplicaciones

JavaScript es un lenguaje de alto nivel que permite la generación de documentos HTML interactivos de un modo sencillo. Dentro de las características de este leguaje se encuentran el responder a pulsaciones del ratón, a las entradas de formularios, a la navegación entre páginas, y a otros eventos.

Este lenguaje resulta de gran apoyo ya que las respuestas a las acciones de los usuarios son invocadas y ejecutadas en el lado del cliente, sin necesidad de hacer uso de la red, lo que evita la sobrecarga de tráfico. Sin embargo también tiene desventajas, una de ellas es que al ser un lenguaje interpretado por los navegadores se eleva el tiempo de ejecución; otra desventaja, y tal vez la más limitante es que su ejecución depende de la capacidad que tenga el navegador para interpretar el código, llegando en el peor de los casos a no ejecutarse.

Los asapectos implementados con apoyo de este lenguaje fueron:

- *Validación de datos de entrada.* Gracias a estas validaciones podemos asegurar la información entrante contra el *Cross-Site-Scripting*, que es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envió de datos sin validación alguna, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el sistema en uso o en el equipo de un usuario.

  Una clave primordial en el campo de la seguridad es no confiar en la entrada de datos de ningún usuario, ya que en cualquier momento estas entradas se pueden convertir en una inserción de código malicioso; es por ello que cualquier aplicación debe validar cada uno de los campos en donde el usuario pueda o le sea requerido el ingreso de datos. Esta validación también se debe aplicar en su correspondiente almacenamiento, ya que cualquier opción de modificación por parte de un usuario se convierte en una entrada potencial de datos erróneos.

Para el caso de los sistemas de información de la DEP-FE la validación de los datos de entrada se realizó mediante scripts JavaScript embebidos en cada página HTML; esta validación se aplica para evitar la inclusión de caracteres conflictivos como -- > ; | .. / \ ‘ = y @ principalmente, siendo ésta última permitida sólo en los correos electrónicos.

- *Manejo de los eventos* también se realizó mediante JavaScript; ésta es una de las funciones más sencillas pero al mismo tiempo de las más potentes a la hora de trabajar con páginas HTML.

- *Programación de acciones*. Acciones asociadas a los eventos del Mouse o a iconos implementados fueron validadas y en algunos casos deshabilitadas para evitar la selección y copiado de una parte o toda la información desplegada.

g) Persistencia de usuarios

Otras de las cuestiones de seguridad que se implementaron fue el manejo de las sesiones.

A diferencia de las *cookies*, que son almacenes de información del lado del cliente (generalmente archivos de tipo texto) que almacenan, administran, crean y borran los navegadores de Internet y que permiten guardar información referente al usuario, sus gustos, preferencias, páginas visitadas, etc., las sesiones son un conjunto de variables almacenadas en el lado del servidor, única por cada entidad que accede a la página web en cuestión y de igual manera ofrece información referente al cliente pero inaccesible a éste.

Las sesiones fueron creadas para almacenar la persistencia de la información relevante de los usuarios que acceden a un sistema; esta información es individual y no requiere ser vista por otras sesiones. Las sesiones tienen cinco métodos principales:

- Abrir sesión
- Definir variable de sesión
- Definir el valor de una variable en sesión
- Obtener el valor de una variable en sesión
- Cerrar la sesión

En los sistemas del SIDEP-FE cada inicio de sesión en los sistemas se validan tanto el usuario como los permisos de acceso a un sistema específico. Una vez autenticado el usuario se establece una sesión para su permanencia dentro del sistema accedido; esta permanencia es llamada en cada página web que sea accesada en el servidor.

4.3.5.4. Seguridad en el Servidor Web

a) Configuración del servidor web

El servidor web es uno de los elementos más importantes en la infraestructura de operación planteada, ya que es a través de éste que se proporcionan servicios de información a la DEP-

FE. La importancia de protegerlo radica en que contiene tanto aplicaciones como información relevante para la institución.

Como primera medida se debe modificar la configuración por default, ya que contiene huecos en la seguridad.

Lo que se modifica en esta configuración es lo correspondiente a la versión del servidor web, correo de administrador, indexación de archivos, directorios públicos y manejo de errores, principalmente. Al deshabilitar o modificar esta información se está protegiendo la configuración del servidor, al mismo tiempo que se proporciona un mínimo de información referente a la versión y configuración del servidor.

Otra de las cuestiones a considerar es mantener una copia de respaldo para reestablecer el ambiente de operación en caso de alguna contingencia; asociado a esto se debe activar el log de transacciones del servidor a fin de realizar un monitoreo de las actividades inusuales.

b) Configuración de Módulo PHP

En este caso se utilizó PHP como lenguaje de programación.

Al igual que el servidor web, el módulo de PHP se debe configurar a fin de proporcionar una protección mínima en cuanto a transmisión y manejo de datos de usuario.

Las principales acciones a realizar es deshabilitar el desplegado de versiones y errores graves del servidor, pues con esto se muestra información propia del servidor.

c) Configuración de los servicios proporcionados

El servidor debe estar configurado especialmente para los servicios que proporciona, entre los que encontramos:

- *Restricción para direcciones IP*. Inicialmente se realizó un filtrado para direcciones propias de la DEP-FE, sin embargo se requirió abrir este filtro al campus, ya que profesores pueden estar fuera de su oficina pero con la necesidad de ingresar a los sistemas.

- *Acceso a archivos y directorios*. El acceso a los archivos y directorios del servidor está restringido para usuarios determinados y con permisos específicos.

- *Administración local y/o remota*. Debe configurarse la administración para realizarse de forma remota en caso de contingencias.

- *Puertos Habilitados*. Se debe deshabilitar todos aquellos puertos que no sean necesarios y sólo dejar aquellos que se requieren para los servicios que proporcione la DEP-FE.

4.3.5.5. Servidor de Base de Datos

a) Configuración del servidor

Cuando se instala el servidor de base de datos también se crea un administrador por default. Debe evitarse el uso de éste para disminuir los ataques y asignarse uno ex profeso, ya que tendrá todos los permisos sobre las bases de datos creadas y asociadas al mismo.

Una vez instalada la base de datos, se deben modificar los permisos de acceso, ya que también por default se permite que cualquiera se conecte al servidor de la base de datos, ya sea de manera local o remota sin solicitar una contraseña de autenticación. En este caso se implementó una cuenta específica para los sistemas, la cual tiene acceso a las bases de datos correspondientes.

Debido a que las conexiones hacia el servidor se transmiten en forma plana, se debe cifrar el canal de comunicación entre el servidor y las conexiones remotas al activar SSL en PostgreSQL. Estas sesiones establecen la asociación entre un cliente y un servidor; son creadas por un protocolo de negociación y definen un conjunto de parámetros de seguridad criptográfica que pueden ser compartidas entre diferentes conexiones, evitándose así el costo de negociar por cada conexión.

b) Respaldos

Se debe generar al menos un par de respaldos de la configuración del servidor a fin de reestablecer el servicio en caso de error, modificación o contingencia cada vez que se modifique y pruebe el correcto funcionamiento de una nueva configuración. De igual manera esta configuración debe ser documentada en el proceso correspondiente.

Uno de los respaldos debe permanecer resguardado por el administrador de los servidores y otro por el responsable del Centro de Cómputo; todo respaldo que se realice debe tener su correspondiente respaldo.

4.3.5.6. Base de Datos

a) Diseño

La seguridad en las Bases de Datos se debe considerar desde el inicio de su diseño, ya que se deben identificar índices, llaves primarias, llaves foráneas y consultas. Todos estos aspectos deben ser congruentes con los procesos de operación de la entidad para la cual se está creando la Base de Datos, en este caso para la División de Estudios de Posgrado de la Facultad de Economía.

Dentro del diseño de la base de datos un aspecto a considerar es el manejo de textos e imágenes. En este caso, se trató de evitar estos tipos de datos por el consumo de recursos que implican.

Para seleccionar un manejador de base de datos uno de los aspectos de mayor peso a considerar es el soporte para la integridad referencial. En este caso particular, se seleccionó Postgres por el soporte a la integridad referencial y por ser un software gratuito.

La base de datos, al ser un componente importante en la operación de los sistemas de información debe estar correctamente documentada mediante un esquema de base de datos indicando todos y cada uno de sus componentes, por lo que cualquier modificación a su diseño debe ser registrada; de igual manera, se debe respetar la nomenclatura definida para los tipos de datos, tablas e índices.

La modificación realizada debe indicar objetivo, solicitante, fecha de operación y tabla o tablas que son afectadas. En este caso en particular, se mantiene actualizada esta documentación.

b) Acceso y procesamiento de la información

El acceso a la información se realizó mediante la programación de sentencias SQL dinámicas. A este respecto cabe aclarar que la referencia a los campos se realizó a través de alias, ya que en caso de presentarse algún problema en la ejecución de sentencias los mensajes de error mostrarán los alias y no los nombres de campo, lo cual daría información de la BD a personas ajenas a la operación y/o entidad.

Las tareas de validación sencillas pueden realizar en el front-end mediante programación PHP o mediante scripts de validación, con lo cual se libera al DBMS.

Se trató de eliminar los tipos de datos de texto debido a potenciales vulnerabilidades que se pueden presentar en su manejo en cuanto a búsquedas y comparaciones, reservando su uso sólo para observaciones o títulos de eventos, principalmente. Otro tipo de valor que se evita es el manejo de campos nulos, ya que con ello sólo se provoca la generación de información incompleta, generando a su vez un mayor tiempo de acceso y de desplegado de información debido al procesamiento que se le debe dar a este tipo de dato.

Otro aspecto a considerar fue la velocidad de respuesta, por lo que ésta se implementó a través del acceso a los campos de manera secuencial, es decir, de acuerdo con el orden en que se encuentran físicamente almacenados en las tablas.

Para el manejo de archivos de imágenes, aún cuando los DBMS permiten el manejo de datos de tipo texto, BLOB, o XML, su manejo no siempre se realiza de manera óptima, por lo que en lugar de almacenar imágenes en la BD, incrementar el tamaño de la BD y tener tiempos de acceso grandes, se almacenan las rutas relativas en las cuales se encuentran almacenadas las imágenes utilizadas por los sistemas de información de la DEP.

c) Accesos a la Base Datos

El acceso a la base de datos se realiza mediante la validación de claves de acceso y roles de usuario.

Para las cuestiones de autenticación se clasificó a los usuarios por grupos: profesores, escolares, jefatura, delegación administrativa, apoyo secretarial y administración de los sistemas.

Otra medida importante es la identificación de acceso y duración del acceso, por lo que a fin de conocer y generar estadísticas de acceso, se registra el ingreso del usuario, así como la fecha, hora y dirección IP del equipo desde donde se realiza la conexión; de esta manera también se tiene el registro de accesos no deseados.

d) Modificación al contenido de la Base de Datos

Hasta ahora la seguridad se ha implementado en tres capas: la primera consiste en la seguridad que implementa el sistema operativo sobre el servidor donde se encuentra el servicio de base de datos, la segunda es tener acceso desde un equipo válido a la base de datos, y por último el acceso a los objetos de la base de datos.

El contenido de la base de datos es lo que se está protegiendo contra accesos no autorizados o contra errores o negligencia en su manejo y actualización, por lo que es de vital importancia conocer quién realiza inserciones o modificaciones a los datos almacenados; es por ello que a estas operaciones se les asocia el registro del usuario que las ejecuta.

Para que un usuario realice una modificación al contenido de la base de datos debe tener los permisos para hacerlo, por lo que se realiza esta validación mediante la programación de scripts, además de las propias validaciones que se realizan mediante las reglas implementadas en la propia base de datos.

e) Criptografía

Debido a que la información que viaja por la red generalmente lo hace en texto plano se vuelve necesario implementar un método criptográfico de protección.

En este caso específico se implementó el algoritmo de encriptamiento MD5, tanto para las claves de acceso como para los datos sensibles en la base de datos.

La característica de este tipo de algoritmos es que se generan en una sola vía con una longitud de 128 bits, y el único ataque que se le conoce es el de investigación exhaustiva; también es muy difícil que dos mensajes distintos produzcan la misma salida.

f) Uso de Certificados

El proceso de obtener un certificado consiste en generar una solicitud de firma de certificado (CSR - Certificate Sign Request), enviar esta solicitud a la Autoridad de Certificación (CA) para que lo apruebe e instalar este certificado en el servidor.

En este caso, el solicitar el certificado a una CA implica un costo, el cual no siempre puede asumir la entidad, como en este caso.

4.3.5.7. Auditorías

a) Auditoría a la base de datos

Aún cuando se implementen mecanismos de seguridad en los canales de comunicación, en las claves de acceso a los sistemas de información y en la propia información almacenada esto no es garantía de que la información almacenada en la base de datos permanece sin alteración alguna.

Es por ello que a fin de mantener la integridad de la información se deben realizar auditorías periódicas para asegurar la integridad de los datos, los tipos de datos utilizados, y los accesos por parte de los usuarios, principalmente.

b) Auditoria a los Equipos de Cómputo

El uso que se les da a los equipos de cómputo es responsabilidad de los usuarios, sin embargo éstos no siempre acatan las políticas de seguridad implementadas, por lo que en cualquier momento se puede realizar una auditoria de la configuración y contenido del mismo a fin de detectar desviaciones sobre las políticas establecidas.

Estas auditorias se vuelven especialmente necesarias cuando se detecta que un usuario está realizando actividades fuera de lo habitual en lo referente a sus atribuciones o se presentan problemas en las relaciones autoridad-subordinado.

4.3.6. Fase 6. Declaración de Aplicabilidad

Esta declaración debe indicar los objetivos, controles seleccionados y los motivos que justifican la selección de éstos, así como las razones por las que otros fueron omitidos. Esto aplica a operaciones, riesgos y personal.

En el presente desarrollo se implementaron controles a nivel operativo, ya que es el ámbito de acción de los sistemas de información.

También de aclara que aunque la metodología indica que se debe desarrollar un apartado para las sanciones en caso de incumplimiento o violación a la Política de Seguridad de la Información definida, en este caso particular se optó por posponerlo debido a la naturaleza de esta entidad académica y al personal que en ella labora.

4.3.6.1. Implementación

En esta primera etapa la implementación de seguridad en los sistemas de información implementó en el análisis y diseño de sistemas, seguridad en el servidor web y seguridad en la base de datos y el servidor correspondiente.

Esta norma recomienda que la organización realice una evaluación de la implementación cada seis meses, aplicando el modelo PDCA (Plan – Do – Check - Act).

4.4. Plan de Recuperación al Desastre

Como se mencionó en el apartado *3.5 Procedimientos y planes de contingencia*, los planes y procedimientos de contingencia están encaminados a conseguir la restauración progresiva y ágil de los servicios asociados a una organización afectados por una interrupción, total o parcial, de su capacidad operativa.

Esta propuesta de Plan de Recuperación al Desastre (DRP, por sus siglas en inglés) se enfoca a la configuración de servidores, a la base de datos y a los programas fuente, que constituyen el soporte para el funcionamiento de los sistemas de información de la DEP-FE.

4.4.1. Análisis de Riesgos

En este caso el análisis del riesgo se realizó en el apartado *4.3.3 Fase 3. Evaluación del riesgo*; donde se definió el riesgo al cual están expuestos los sistemas de información de la DEP-FE, así como las medidas preventivas y correctivas realizadas para la protección de los activos asociados.

4.4.2. Actividades a realizar

Las actividades a realizar deben estar documentadas y claramente definidas mediante acciones y procedimientos para cada etapa en el proceso de restauración, respetando siempre las políticas de seguridad previamente establecidas; mientras que las políticas definidas indican el "qué hacer", los procedimientos indican el "cómo hacer", ya que se indica de manera puntual cada actividad, la secuencia en que se debe realizar y el responsable de su ejecución.

Estas actividades involucran directamente al personal de la DEP-FE, pues se realizan antes, durante y/o después de la ocurrencia de la falla.

4.4.2.1. Actividades Previas al Desastre

Las actividades previas al desastre están enfocadas a contrarrestar los posibles ataques que puedan sufrir los sistemas de información al operar de manera cotidiana; se asume que las políticas de seguridad definidas se encuentran correctamente implementadas y el personal capacitado.

Antes de cualquier eventualidad en los sistemas de información se debe establecer un plan de acción, el cual debe tener documentados los procedimientos relativos a:

a) Sistemas de información de misión crítica

La DEP-FE ha generado una relación de los Sistemas de Información con que se cuenta identificando toda información, sistematizada o no, que sea necesaria para la operación institucional indicando las áreas generadoras y usuarias de cada sistema (Tabla 4-11).

Sistema	Plataforma de Desarrollo	Generador de información	Área Usuaria	Periodo crítico
Sistema de Información de la Jefatura de la DEP-FE	Servidor web, PHP, Postgres	- Jefatura de la DEP-FE - Consejo Técnico	- Dirección de la FE - Jefatura de la DEP-FE - Secretaría de Planeación	- Diario - Mensual - Trimestral - Semestral - Anual
Sistema de alumnos de Doctorado en Economía	Servidor web, PHP, Postgres	- Sección Escolar	- Dirección de la FE - Jefatura de la DEP-FE - Sección Escolar - Coordinación del Programa de Posgrado en Economía (PPE)	- Mensual - Trimestral - Semestral - Anual
Sistema de alumnos de Maestría en Economía	Servidor web, PHP, Postgres	- Sección Escolar	- Dirección de la FE - Jefatura de la DEP-FE - Sección Escolar - Coordinación del PPE	- Mensual - Trimestral - Semestral - Anual
Sistema del Programa Único de Especializaciones en Economía	Servidor web, PHP, Postgres	- Programa Único de Especializaciones en Economía - Consejo Técnico	- Dirección de la FE - Jefatura de la DEP-FE - Secretaría de Planeación	- Mensual - Trimestral - Semestral - Anual
Sistema de la Coordinación del Programa de Posgrado en Economía	Servidor web, PHP, Postgres	- Coordinación del PPE - Jefatura de la DEP-FE - Tutores	- Dirección de la FE - Jefatura de la DEP-FE - Sección Escolar - Coordinación del PPE	- Diario - Mensual - Trimestral - Semestral - Anual
Sistema de Inventarios	FoxPro	- Área de Bienes y suministros	- Jefatura de la DEP-FE - Centro de Cómputo de la DEP-FE - Área de Bienes y Suministros	- Semanal - Mensual - Semestral - Anual

Tabla 4-11. Sistemas de Información de Misión Crítica de la DEP-FE

b) Equipos de Cómputo

Los equipos de cómputo deben estar señalizados, tanto en registro electrónico como de manera física para que en caso de un eventual desalojo se conozca su prioridad para salir de las instalaciones. La prioridad está indicada como alta, media y baja, y depende de la importancia del equipo para continuar con las actividades propias de la DEP-FE (Tabla 4-12).

Este registro de importancia de los equipos siempre debe estar actualizado indicando el software instalado, la configuración específica para cada equipo y el o los servicios que proporciona.

Equipo	Servicio	Prioridad
Servidor DEPFE-EDU	Servidor Web Página de profesores Sistemas de Información de la DEP-FE Plataforma educativa Moodle	Alta
Tcnicos2	Sistema de Inventarios	Alta
Jefatura1	Documentación de la Jefatura de División	Alta
CenCo	Documentación del Centro de Cómputo	Alta
Especializaciones	Programa de Especializaciones	Alta
Jefatura2	Plataforma de Desarrollo Currícula de la Planta Académica	Alta
Jefatura3	Circulares, Memoranda, documentos de la DEP-FE	Media
Planta Académica	Investigaciones, desarrollo de material didáctico	Media
Ayudantes de Profesor	Investigaciones, documentación personal	Media
Apoyo secretarial	Documentos de apoyo, personales	Baja
Laboratorio de Econometría	Paquetes estadísticos	Baja
Sala de Trabajo	Paquetes estadísticos	Baja

Tabla 4-12. Priorización de Equipos de Cómputo

Como se puede observar sólo los equipos directamente asociados con el desarrollo y operación de los sistemas de información, así como los que almacenan información necesaria para la jefatura de la DEP-FE tienen una prioridad alta; respecto a los equipos asociados a investigadores, profesores y ayudantes de profesor periódicamente se realiza un respaldo de su contenido, por lo que siempre se tendrá un respaldo bajo resguardo, generalmente en poder del propio académico; los equipos de apoyo secretarial, de la sala de trabajo y los del laboratorio tienen una prioridad baja ya que la información almacena en ellos no es de vital importancia para la continuidad en las operaciones de la DEP-FE, sólo es de apoyo para las necesidades propias de los estudiantes.

c) Obtención y almacenamiento de respaldos de información

Se debe respetar la política para generar respaldos de información y resguardo de los mismos.

Se debe contar con un documento donde se especifica la configuración de cada servidor (Anexo 3): sistema operativo, servidor web, servidor de base de datos, y de la propia base de datos a fin de

reproducir la plataforma de operación de los sistemas de la DEP-FE en caso de contingencia, considerando como de igual importancia los programas fuentes y objeto de dichos sistemas.

d) Formación de equipos operativos

La formación de equipos operativos tiene por objetivo la ejecución del plan de recuperación a desastres. Aunado a la formación de estos equipos se debe designar un responsable general de la seguridad de la información, el cual deberá coordinar y/o ejecutar las actividades relativas a:

- Capacitar y apoyar en la generación de respaldos de información a todo el personal de la DEP-FE.
- Planificar y establecer los requerimientos de los sistemas de información en cuanto a versiones de sistema operativo, configuración de servidores, equipos que los soportan.
- Supervisar los procedimientos de respaldos y restauración.
- Supervisar el funcionamiento de la infraestructura de comunicaciones.
- Organizar las pruebas de hardware y software.
- Ejecutar los trabajos de recuperación.
- Participar en las pruebas y simulacros de desastres.

En este caso el responsable de estas actividades es el responsable del Centro de Cómputo, el cual realiza la supervisión y coordinación de las actividades técnicas anteriores al mismo tiempo que es el enlace con el Centro de Cómputo de la Facultad de Economía, el cual controla y administra la red interna de la Facultad.

El equipo de recuperación al desastre se encuentra integrado, en orden de responsabilidad, como se indica en la Tabla 4-13.

Cabe aclarar que aún cuando los números telefónicos particulares es considerada información confidencial, en el directorio de los integrantes de los equipos operativos debe incluirse tanto números telefónicos del domicilio como el del móvil. Este directorio deberá estar actualizado y bajo resguardo del jefe la División de Estudios de Posgrado con el fin de garantizar que siempre exista alguien a cargo, y que pueda ser contactado en caso de presentarse una contingencia. Este equipo debe estar en constante coordinación en todas las actividades del DRP.

Otro elemento importante, aunque no directamente asociado a los sistemas de información, es el Delegado Administrativo quien se encargará de la supervisión de las instalaciones físicas del edificio y de los bienes en él contenidos.

Cargo	Nombre	Domicilio	Número telefónico de contacto	Número celular de contacto
Jefe de la División				
Secretario Académico				
Responsable del Centro de Cómputo				
Administrador de Servidores				
Desarrollador de Sistemas de Información				
Usuarios de los sistemas e infraestructura				
Delegado administrativo				

Tabla 4-13. Formato para personal esencial en caso de contingencia

e) Identificación de soluciones

Incluyen las fallas de los sistemas u otros eventos que hacen evidente la necesidad de implementar el plan de contingencia. Estas actividades están identificadas también en la sección de evaluación del riesgo anteriormente desarrollado.

Dentro de las actividades a realizar podemos mencionar

- Asignación de equipos de solución para cada función, área funcional o área de riesgo de la organización.
- Comparar los riesgos y determinarles peso respecto a su importancia crítica en térmico del impacto de los mismos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- Revisión de la factibilidad de las soluciones y las reglas de implementación.
- La definición e identificación de equipos de acción rápida o equipos de intensificación por área funcional o de negocios de mayor importancia.

f) Matriz de análisis de riesgos

A continuación se presenta una matriz de riesgo para los eventos que pudieran ocurrir con mayor frecuencia.

Impacto				
	Alto	Ausencia de respaldos	Ausencia de autenticación y registro de usuarios	Ausencia de Firewall
	Medio	Ausencia de servicio de red	Personal sin capacitación especializada	Errores de diseño de la BD
	Bajo	Robo de equipo de usuarios	Fallas en la corriente eléctrica	Existencia de virus o spyware en los equipos
		Baja	**Media**	**Alta**

Probabilidad

Figura 4-4. Matriz de Análisis de Riesgos

4.4.2.2. Actividades Durante el Desastre

Las actividades dependerán de la naturaleza del desastre y del horario en que se suceden, por lo que cuando ocurra una contingencia, es esencial que se conozca a detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Recordemos que en el análisis de vulnerabilidades, amenazas y riesgos se especificaron las medidas preventivas mediante las cuales se minimiza el riesgo, de tal manera que se proteja el activo y principalmente la información procesada.

Si bien este Plan nos permite conocer qué actividades se debe realizar y cuál es su secuencia, el tiempo de respuesta dependerá de la contingencia y del impacto que ésta produzca, por lo que en principio se establece un plazo máximo de dos días para la recuperación total en caso de un error en los sistemas de información.

a) Casos que pudieran ocurrir con mayor frecuencia

Fallas en la corriente eléctrica

Por corto circuito. El UPS mantendrá activos los servidores y, si es el caso, algunos equipos conectados a la red. Esto será por el tiempo que dure la batería y en espera de que se repare la avería.

Por ausencia de suministro eléctrico. Los UPS proporcionarán la corriente de emergencia necesaria para que los usuarios completen sus operaciones de cierre de aplicaciones y apagado de equipos hasta que se restituya dicho suministro. Estos procesos no deben consumir más de 15 minutos.

Ausencia de servicio de red

Revisar la conexión a la red.
Revisar la configuración del equipo.
Revisar las conexiones de red de los equipos contiguos.
Notificar al responsable del centro de cómputo.

Revisar que los servidores estén funcionando.
Revisar que las aplicaciones estén funcionando.
En caso de seguir sin servicio notificar al personal responsable de la red en el Centro de Informática de la Facultad de Economía.
Revisar el switch del posgrado.
Reiniciar el equipo.
Validar la correcta configuración de los servidores.
Validar la existencia del servicio en todos los equipos.

Ausencia de servicio web

Notificar al administrador de los servidores.
Revisar la configuración.
Revisar los logs de transacciones.
Identificar comportamientos inusuales en el log.
Dar de baja los procedimientos incompletos o corruptos.
Realizar las modificaciones necesarias, si es el caso.
Realizar las correcciones, si es el caso.
Reinicializar el servidor.
Reinicializar los procesos básicos del servidor.
Verificar que los servicios funcionen correctamente.

Errores en la base de datos

Validar tipos de datos en las tablas.
Validar la integridad referencial.
Darle seguimiento al error encontrado.
Realizar la modificación/corrección necesaria.

Robo de equipo de cómputo

Notificar de manera inmediata al delegado administrativo.
Notificar a los vigilantes del edificio.
Realizar una búsqueda del equipo en todas las áreas comunes donde pudiera haber sido dejado.
Revisar los cubículos y áreas académicas a fin de corroborar que no exista otro robo.
Notificar al abogado de la Facultad a fin de levantar el acta correspondiente.
Buscar y tener los resguardos del equipo que fue sustraído.
Actualizar los registros de equipo de cómputo indicando la baja.

b) Cronograma de recuperación

Componente	Secuencia			
Red				
Servidores				
BD				
Aplicaciones				

c) Matriz de planificación de contingencia

En este caso, casi todas las tareas que se realizan mediante los sistemas de información pueden ser realizadas de manera manual apoyados en herramientas de oficina, tal como se indica en la Tabla 4-14, y se recurrirá a los registros en papel que constantemente se emiten.

Proceso estratégico en contingencia	Respuesta al incidente	Tiempo de respuesta
Informe de actividades	Procesamiento en excell Conteo manual Revisión de informes previos	Inmediato
Estadísticas de alumnos	Revisión de expedientes Conteo manual	Inmediato
Corrupción de la base de datos	Revisión de expedientes Revisión y/o modificación de la BD al implementar la integridad referencial Adicionar este procedo de verificación a los procesos de auditoria establecidos	Inmediato
Generación de constancias	Procesamiento en paquetes gráficos Procesamiento en Word	Al menos un día
Convocatoria de CONACyT	Revisión de expedientes Revisión de registros impresos	Al menos un día

Tabla 4-14. Matriz de planificación de contingencias

4.4.2.3. Actividades Posteriores al Desastre

Las actividades a realizar están enfocadas a la resolución de la contingencia presentada, así como la protección a futuro de los activos comprometidos en esta contingencia.

La secuencia a seguir en estas actividades se presenta a continuación.

a) Evaluación de daños

Esta evaluación estará enfocada a tiempo y dinero invertido, tanto en la solución como en las pérdidas sufridas por la contingencia.

Se deberá valorar la implementación de nuevos mecanismos que permitan realizar una mejor vigilancia tanto de los procesos como del personal asociado a los mismos.

b) Priorización de actividades del Plan de acción

Cada que ocurre una contingencia se revisa el plan de acción para corroborar que las actividades y secuencia de las mismas es el correcto. En caso contrario se deberá realizar un reacomodo y/o incremento de las actividades a fin de cubrir los nuevos eventos que pueden afectar el funcionamiento de los sistemas de información.

También se deberá actualizar el registro de contingencias a fin de determinar el área con mayores incidentes y personal involucrado en los mismos, esto para detectar puntos rojos en la administración de la seguridad y para identificar a personal que omite, intencionalmente o no, las políticas de seguridad establecidas.

c) Ejecución de actividades

Una vez modificado el Plan de acción se debe implementar y probar en el ambiente de pruebas a fin de determinar que han sido correctas las modificaciones y que realmente se cubren las nuevas necesidades de seguridad.

d) Evaluación de resultados

La evaluación de resultados siempre se hace necesaria ya que no basta con modificar el plan, sino revisar los resultados para evitar que se cancelen servicios previamente probados y validados.

e) Retroalimentación del Plan de Acción

Este Plan de acción debe ser actualizado y retroalimentado cada que se presente y contrarreste una contingencia, a fin de tener actualizados los procedimientos a seguir.

Por otro lado, tampoco basta con documentas los procedimientos a realizar, sino que se tienen que dar a conocer al personal directamente involucrado, así como al resto del personal para que conozcan los caminos de comunicación y las personas responsables de la solución para cada problema específico que se presente.

Todas estas actividades están encaminadas a la retroalimentación del modelo de seguridad implementado. Recordemos que en todas las actividades asociadas a la seguridad debemos seguir el modelo PDCA (Plan – Do – Check - Act).

5. Resultados y Beneficios de la Implementación

Durante el estudio del nivel actual de seguridad en la DEP-FE se encontró que existe un nivel de seguridad mínimo en los equipos de usuarios, en los laboratorios y salas de cómputo, así como en los sistemas de información que se operan.

Esta deficiencia tiene como consecuencia una alta vulnerabilidad en los procesos de operación y en la información que se maneja.

El presente trabajo dio como resultado la clasificación de activos con sus respectivas vulnerabilidades y amenazas a enfrentar, lo que derivó en un análisis de riesgos (Ver 4.3.3. Fase 3. Evaluación del riesgo); a partir de este análisis se generó un programa de seguridad inicial donde se clasificó a dichos activos tomando como base la importancia de la información que generan, administran y/o almacenan.

El valor de los activos a proteger se determinó por la importancia de la información que manejan y por el impacto que pudiera tener su ausencia dentro de la organización, el cual puede ser desde la destrucción del equipo hasta la pérdida de la propia información; recordemos que cualquier control que se implemente debe basarse únicamente en el valor del equipo y los servicios que proporciona.

En esta primera etapa de aseguramiento se definieron criterios e implementaron controles de seguridad específicos para los activos seleccionados, entre los que se encuentran mecanismos de validación y protección de datos en los sistemas de información reduciendo con ello la posibilidad de error o negligencia en su manejo por parte de los usuarios, así como una configuración especializada en los servidores que dan soporte a la infraestructura de operación de los sistemas de información.

A través de esta definición de criterios se generó una Política de Seguridad de la Información para la DEP-FE a fin de ponerla en práctica y de esta manera mantener la integridad, confiabilidad y disponibilidad de la información reduciendo el riesgo de pérdida o modificación no autorizada de la misma.

5.1. Sistemas de Información para la DEP-FE

Para proteger la información utilizada y almacenada por los sistemas de información de la DEP-FE, durante su desarrollo e implementación se siguieron los procedimientos y recomendaciones para un desarrollo seguro, lo cual aún cuando no es garantía de tener un sistema totalmente seguro sí reduce las posibilidades de ataque y generación de daño.

En los sistemas de información se implementaron mecanismos de validación de datos, establecimiento de sesiones de usuario, encriptado de datos en la base de datos, así como el registro de las operaciones que realizan los usuarios dentro de los sistemas, principalmente. Sin embargo esto no es garantía total, por lo que también se abordaron cuestiones asociadas a nuevas amenazas y aspectos relacionados con la ingeniería social.

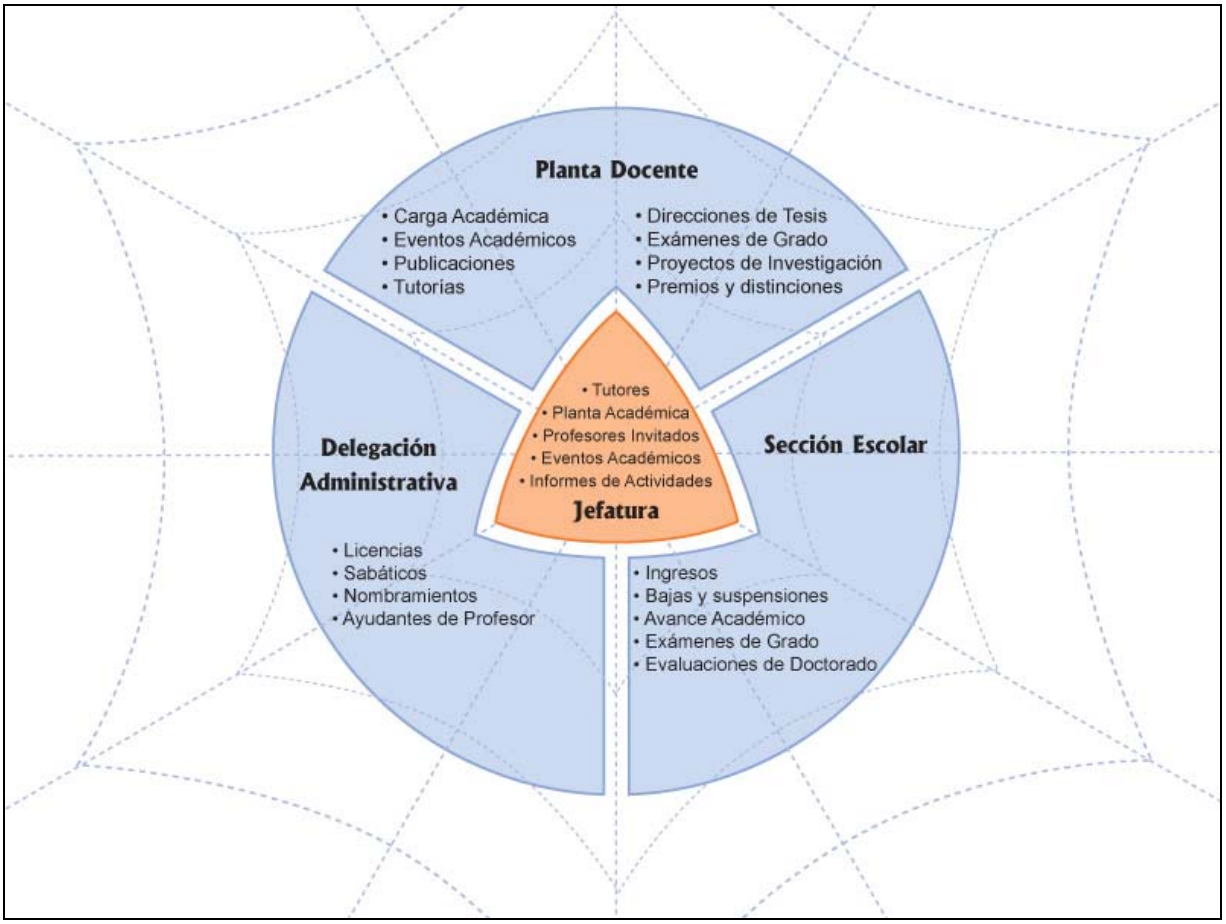

Figura 5-1. Sistemas de Información de la División de Estudios de Posgrado de la Facultad de Economía

Mediante la configuración especializada de los servidores y la base de datos también se protege a la información y se evitan ataques que puedan llegar a poner en riesgo la integridad de la información.

5.2. Política de Seguridad de la Información para la DEP-FE

PRESENTACIÓN

El propósito de establecer una Política Global de Seguridad de la Información para la División de Estudios de Posgrado de la Facultad de Economía es el proteger la información, los sistemas de información, y los activos de esta entidad académica haciendo énfasis en la confidencialidad, integridad y disponibilidad de la información

Mediante esta Política Global de Seguridad de la Información se pretende determinar las responsabilidades de los usuarios y su ámbito de acción, así como concientizar y sensibilizarlos en cuanto al manejo de la información dentro de su área de trabajo.

Esta política de seguridad surge del análisis de riesgos y escaneo de vulnerabilidades realizada a la División de Estudios de Posgrado de la Facultad de Economía, y pretende aportar los elementos necesarios que ayuden a administrar los riesgos detectados mediante la implementación y mejora continua de políticas específicas para la prevención de incidentes y así minimizar su posible impacto.

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Todo el personal (investigadores, académicos, alumnos, empleados y usuarios) de la División de Estudios de Posgrado de la Facultad de Economía debe laborar dentro de un ambiente de trabajo en el que se garantice la confidencialidad, integridad y disponibilidad de la información materia de su trabajo.

Para ello se deben llevar a cabo las acciones necesarias que permitan mantener estas características de la información en un mínimo aceptable, por lo que las siguientes acciones deben ser respetadas y acatadas por todo el personal antes indicado.

Esta política se aplica a todos los equipos de escritorio, servidores, redes, y sistemas de información pertenecientes o manejados por la División de Estudios de Posgrado de la Facultad de Economía. La política cubre únicamente la información manejada por los equipos de escritorio y la red interna.

OBJETIVO

Proteger la información a nivel físico, lógico, logístico y humano mediante lineamientos de planeación que permitan el diseño e implementación de un modelo de seguridad que genere un mejoramiento continuo y dinámico asegurando con ello la continuidad en la operación de la División de Estudios de Posgrado de la Facultad de Economía.

VIGENCIA

Esta Política de Seguridad entrará en vigor a partir de que sea aprobada por el H. Consejo Técnico de la Facultad de Economía, y sea publicado en su órgano oficial de divulgación (Gaceta Economía).

ROLES Y RESPONSABILIDADES

Roles en el Manejo de la Seguridad de la Información

» El Centro de Cómputo es responsable de establecer y mantener la política de seguridad en los equipos de escritorio, así como de las directrices y procedimientos de operación de los mismos.

» La Jefatura de la División, a través del responsable del desarrollo de sistemas de información, es la responsable de asegurar el cumplimiento de las políticas referentes a las tecnologías de la información, y a los procedimientos de actualización de la misma.

» El Centro de Informática de la Facultad de Economía tiene bajo su responsabilidad el monitoreo de accesos no autorizados a la red y otros incidentes de seguridad de la información.

» La acción disciplinaria en respuesta a las violaciones de las políticas de seguridad de la información es responsabilidad del Jefe de la División en conjunto con la Delegación Administrativa correspondiente y el departamento de Personal de la Facultad de Economía.

Responsabilidades

a) Usuario
Se requiere que los usuarios se familiaricen con la política de seguridad de la información, procedimientos, normas y legislación aplicable. Deben entender claramente estas exigencias y cumplir con ellas.

b) Responsables de la información
- Los responsables de la información son los directivos que requieren adquirir, desarrollar y mantener sistemas de información que apoyen en la toma de decisiones y otras actividades de la organización.
- Cada sistema de información, así como los procesos asociados deben tener un responsable designado.
- Los responsables de la información están obligados a indicar la clasificación que mejor refleje la naturaleza de cada tipo de información: sensible, de valor crítico y disponibilidad de la misma; esta clasificación determinará el nivel de acceso de los usuarios.

c) Administradores de la información
   - Se denomina administradores al personal que se encargan de la custodia de la información de la organización o la información confiada a la organización y almacenada en computadores personales y servidores; este personal puede ser personal de desarrollo, administradores de sistemas o usuarios de los mismos.
   - Cada sistema de información debe tener al menos un administrador autorizado. Los administradores son responsables del almacenamiento de la información, la aplicación de sistemas de control de acceso (para evitar la divulgación no autorizada) y ejecución periódicamente de copias de seguridad (para asegurar que la información crítica no se pierda).
   - Los administradores también están obligados a desarrollar, aplicar, mantener y revisar las medidas de seguridad definidas por los dueños de la información

CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información constituye un elemento importante para la gestión de riesgos, ya que determina las necesidades, la prioridad y el grado de protección necesarios. La información, los sistemas y procedimientos que la manejan deberán integrarse en una de las siguientes categorías:

a) Privada
   La información privada es aquella que sólo interesa a su dueño, al desarrollador o al investigador en cuestión; no debe ser dada a conocer.

b) Sólo para uso interno
   Se considera información de uso interno a aquella que debe estar disponible solamente para un conjunto determinado de personas; debe ponerse un cuidado especial en información que por ley o que por políticas de la propia Facultad de Economía debe permanecer confidencial.
   La clasificación de un recurso como de uso interno deberá incluir los criterios para determinar quiénes tienen acceso a él. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red externa deberán tomarse medidas de seguridad extremas.
   La pérdida o no disponibilidad de la información puede ocasionar un daño en los activos de la Entidad Académica, de ahí la importancia de su protección.

c) Confidencial
   Se considera como recurso confidencial a todo aquel que sólo deberá utilizarse y ser del conocimiento de los miembros de la Entidad Académica, y por defecto todo aquel recurso que no haya sido explícitamente clasificado como disponible al público.
   Es la información que, en poder de personas no autorizadas compromete los intereses particulares de la Entidad Académica o de sus miembros.

d) Pública
   Se considera como información público aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado por parte de los directivos como de dominio

público; está disponible para quien lo solicite (mediante los canales autorizados) o mediante su publicación en órganos informativos.

Esta clasificación deberá ser documentada e informada a todo el personal de la entidad, y deberá evaluarse y actualizarse periódicamente. De igual manera, deberá existir un responsable en cada área de la entidad que responda por la información clasificada como pública.

POLÍTICAS DEFINIDAS

Las políticas de seguridad definidas están orientadas a proteger la integridad, confidencialidad y disponibilidad de la información, a fin de proporcionar la continuidad en la operación de la División de Estudios de Posgrado de la Facultad de Economía.

Políticas para la Seguridad Física

Acceso al edificio
» Contar con mecanismos de control que permitan asegurar que el personal que ingrese a las instalaciones de la DEP-FE tenga la autorización correspondiente. » Mantener vigilancia constante mediante rondines a las diversas áreas del edificio que alberga a la División de Estudios de Posgrado.

Control de acceso y salida de paquetes
» Los vigilantes del edificio serán los encargados de llevar un control de acceso y salida de paquetes. » Realizar una revisión de bultos o paquetes sospechosos o de aquellos cuyas dimensiones sean mayores a los de una mochila de estudiante. » En caso de ingreso de paquetes de dimensiones grandes, deberá registrarse su contenido, área destino, persona receptora y responsable del mismo.

Acceso a Cubículos
» El acceso a los cubículos se realizará de forma controlada y bajo la responsabilidad del profesor o investigador asignado al mismo. » Es responsabilidad del profesor, académico o investigador el control de las copias de llaves de acceso a su cubículo, excepto la correspondiente al personal de intendencia. » Se debe mantener vigilancia remota de los cubículos mediante cámaras de seguridad a fin de determinar actividades sospechosas o personal no autorizado en estas áreas.

Suministro eléctrico
» El suministro eléctrico debe estar garantizado para el correcto funcionamiento de los equipos de cómputo. » En caso de interrupción de la energía eléctrica, todos los usuarios deben guardar su información, realizar las copias correspondientes, y apagar los equipos que estén en uso a fin de evitar cualquier pérdida de información.

» Cada equipo de escritorio debe contar con un UPS que proporcione energía suficiente para poder almacenar la información y apagar el quipo.

Cableado estructurado

» El cableado debe seguir las normas de operación internacionales a fin de garantizar el funcionamiento correcto de la red interna.
» Llevar a cabo una revisión periódica y contar con protecciones contra ruidos e interferencias electromagnéticas, a fin de realizar las acciones correctivas necesarias.
» Documentar, mediante planos, la estructura del tendido de cables y conexiones de red existentes.
» Mantener oculta la línea de tendido de cableado evitando acciones vandálicas o malintencionadas.

Seguridad de los equipos de escritorio

» Contar con equipo apropiado de seguridad física (extintores, aire acondicionado, energía regulada, etc.) para evitar daños tanto a la información como a los equipos.
» Dotar de equipo UPS a los equipos que efectúen operaciones críticas dentro de la organización a fin de proporcionar continuidad a las operaciones.
» Proteger a los servidores de aplicaciones contra robo de partes.
» Establecer un área segura y acondicionada para los servidores de aplicaciones críticas.
» Generar discos de arranque para los equipos considerando el sistema operativo, libre de virus.

Acceso al Área de Servidores

» Restringir el acceso a toda persona ajena al área a fin de reducir el riesgo de accidentes o actividades fraudulentas.
» Prohibir el acceso y permanencia de toda persona ajena al área de servidores cuando el responsable de dicha área no esté presente.

Seguridad en los Laboratorios y Salas de Cómputo

» Los laboratorios y salas de cómputo deberán contar con un registro de ingreso y egreso de usuarios indicando nombre, número de cuenta, hora de inicio, hora de término y actividad realizada.
» Los dispositivos de almacenamiento externos utilizados en estas áreas deberán ser previamente revisados por personal del Centro de Cómputo y, si es el caso, saneadas de cualquier virus o malware reconocido por la vacuna utilizada por dicho centro.
» Los laboratorios de cómputo sólo podrán ser utilizados previa solicitud, y deberán ser revisados físicamente antes y después del préstamo a fin de asegurar la permanencia del equipo de cómputo dentro de los mismos.
» Los ingresos a la sala de cómputo deberán ser controlados por personal del Centro de Cómputo a fin de asegurar la permanencia de los equipos de cómputo y su óptimo funcionamiento.

Seguridad en los Escritorios
» Cualquier bien informático utilizado en el área de escritorio debe estar resguardado cuando el usuario responsable se encuentre fuera de su sitio de trabajo a fin de evitar intrusiones y robo de información. » Evitar dejar documentos con información clasificada como confidencial, privada o de uso interno en los escritorios a la vista de cualquier persona. » Resguardar en gabinetes con llave todo documento con información privada y/o confidencial. » Llevar el registro de la información solicitada por áreas distintas a la propietaria. » Llevar un registro de expedientes que salen del área responsable indicando información proporcionada, quién lo solicita, fecha de préstamo y fecha de devolución.

Seguridad en equipos de Fotocopiado y Fax
» Establecer y utilizar áreas específicas para estos servicios. » Llevar un control de fotocopias y faxes enviados por cada usuario. » Evitar la atención de servicios de manera simultánea. » Revisar el trabajo que se entrega a cada usuario a fin de evitar fugas de información o entregas incorrectas. » Mantener la continuidad de estos servicios, de tal manera que en caso de ausencia del responsable del servicio la Unidad Administrativa designará a un elemento que lo sustituya y continúe proporcionándolo.

Registro de Inventario
» Registrar todo equipo que sea asignado a la División de Estudios de Posgrado de manera inmediata a su asignación. » Registrar todos los cambios en componentes, actualizaciones y responsables de los equipos de cómputo. » Realizar una revisión física de los equipos de cómputo, componentes e inventarios registrando los resultados obtenidos.

Mantenimiento de los equipos de cómputo
» El servicio de mantenimiento se dará a todos los equipos que la DEP-FE, excepto aquellos que aún cuentan con garantía del proveedor en cuyo caso se enviarán con el mismo para su mantenimiento. » Para el caso en que la póliza de garantía haya expirado, personal del Centro de cómputo tratará de realizar la reparación; en caso de no ser posible, el equipo se enviará a talleres especializados. » Realizar mantenimiento preventivo al equipo de cómputo de manera periódica y por lo menos una vez al año. » Prestar especial atención al mantenimiento preventivo a los servidores de aplicaciones. » Mantener un registro de averías para cada equipo de cómputo indicando origen, fecha de ocurrencia, tratamiento y responsable de la solución. » Los servicios de mantenimiento correctivo se realizarán con la siguiente prioridad: académicos, administrativos y alumnos.

Políticas para la Seguridad Lógica

Segmentación de la red
» Se debe realizar una segmentación en base a las áreas de servicio, interrelación entre ellas y los productos obtenidos por las mismas. » Se debe documentar de forma detallada los diagramas de las redes, tipos de enlace y ubicación de nodos.

Instalación y configuración de firewalls y proxies
» Se debe configurar el firewall de manera que se prohíba todos los protocolos y servicios, habilitando únicamente los requeridos (postura de negación preestablecida). » Se debe asegurar que la totalidad del tráfico de la red interna sea filtrado y controlado por un firewall prohibiendo el tráfico que no se encuentre expresamente autorizado. » Se debe configurar un firewall personal en cada equipo de misión crítica.

Administración de la red
» El Centro de Cómputo debe contar con un inventario de todos los componentes de la red, así como de los sistemas, aplicaciones y activos de información que estén asociados a la red interna de la DEP-FE. » Se debe configurar de forma específica los dispositivos de la red a fin de proporcionar una protección mínima. Esta configuración debe ser actualizada de manera periódica. » Se debe contar con un plan de mantenimiento preventivo constante a los componentes de la red de acuerdo con los requerimientos del fabricante » Se debe realizar un monitoreo constante de la red a fin de medir el desempeño de la misma y atender las fallas detectadas. » La conectividad a Internet será otorgada para propósitos relacionados con funciones académicas o de investigación y mediante autorización del Centro de cómputo de la DEP-FE. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior. » Los sistemas de información deben ser utilizados exclusivamente para fines profesionales. » Se debe realizar el bloqueo de sitios web que nada tengan que ver con las operaciones de la DEP-FE. » Se debe asegurar la integridad, disponibilidad y confidencialidad de la información transmitida por la red ya sea a través de los dispositivos de hardware, los protocolos de comunicación o de controles específicos.

Antivirus
» Se debe instalar en cada equipo de cómputo el software antivirus evaluado y proporcionado por el Centro de Cómputo de la DEP-FE. » Se debe capacitar a los usuarios en la actualización del antivirus en sus equipos. » Se debe capacitar a los usuarios en la ejecución de revisión y limpieza de sus equipos. » Programar escaneos periódicos en las salas de trabajo, laboratorios de cómputo y áreas de acceso común realizando la limpieza de virus, en caso de existir.

» Mantener un disco de emergencia con una copia del antivirus más reciente.

Dispositivos de los equipos de escritorio

» Asignar un password de administración del BIOS en cada equipo, el cual deberá ser asignado y administrado por el Centro de Cómputo de la DEP-FE.
» Deshabilitar las disqueteras y lectores de CD en aquellos equipos donde no se necesiten.
» Cualquier equipo o dispositivo externo que no se encuentre en uso deberá permanecer resguardado bajo llave en las áreas del Centro de Cómputo de la DEP-FE.

Autenticación

» Todos los sistemas de información desarrollados por personal de la DEP-FE deberá solicitar, para el acceso, un nombre de usuario, un password, y presentar la opción para cambiar estos datos.
» Se debe utilizar máscaras para todas las contraseñas ingresadas por el usuario a fin de no ser mostradas en pantalla.
» Se debe presentar el nombre de usuario en cada sistema una vez validada la identidad del usuario.
» Se debe encriptar los datos de autenticación mientras son transmitidos a través de la red.
» Cada sistema de información de la DEP-FE debe realizar un registros de intentos fallidos.

Passwords

» Los passwords utilizados por el personal de la DEP-FE deben tener una longitud mínima de 6 y máxima de 15 caracteres.
» Los passwords deben contener una combinación de letras y números.
» Se debe solicitar el cambio de password al menos cada seis meses o en periodos más cortos de manera automática.
» Se debe bloquear el perfil de usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas.
» El usuario podrá modificar su password cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.
» Se debe almacenar los últimos cinco passwords de usuario a fin de evitar su repetición.
» El almacenamiento de passwords de usuario se realizará de manera encriptada a fin de evitar su robo o mal uso.
» El proporcionar el password a un tercero es total y absoluta responsabilidad del dueño de la cuenta, con su consecuente sanción.

Sesiones de usuario

» Todo sistema de información desarrollado por personal de la DEP-FE debe tener implementado el manejo de sesiones de usuario.
» Se debe evitar dejar sesiones de trabajo abiertas cuando el responsable del equipo de

cómputo abandone su sitio de trabajo.
» Se debe cerrar la sesión de un usuario de manera remota si el sistema no registra actividad por un lapso de quince minutos.

Administración de controles de acceso

» Todos los sistemas desarrollados para la DEP-FE debe contar con una matriz de control de acceso para cada usuario/servicio.
» Se debe realizar una validación de desplegado de información sólo para un usuario válido y para el módulo en cuestión.

Políticas para la Seguridad en los Sistemas de Información

Análisis de Sistemas de Información

» Utilizar metodologías formales de desarrollo.
» Realizar un levantamiento de requerimiento a todos los niveles: directivo, operativo y técnico.
» Llevar a cabo la separación entre actividades operativas, mecánicas y automatizables.
» Identificar a los usuarios y roles de cada uno.
» Generar un modelo conceptual por cada sistema de información a desarrollar.
» Se debe considerar las cuestiones de seguridad desde la etapa de análisis de cualquier desarrollo de sistema de información.

Desarrollo de Sistemas de Información

» Los desarrollos realizados por personal de la DEP-FE deberán utilizar herramientas de software libre.
» Se debe desarrollar los sistemas de información por etapas validando cada una de ellas.
» Se debe implementar controles que validen los tipos de datos de entrada.
» Respetar los estándares de programación como identificación de variables, módulos y procesos.
» Establecer una estructura de directorios para las opciones de los sistemas.
» Llevar un control de versiones del desarrollo de sistemas de información.
» Deberá existir un ambiente de desarrollo por cada sistema de información, el cual debe ser distinto al ambiente de operación.
» Las diversas operaciones a realizar por los sistemas deben ser probadas de manera exhaustiva a fin de evitar errores de operación.
» No debe existir herramientas de desarrollo en el ambiente de operación de los sistemas de información.
» Se debe mantener un respaldo de los programas fuente del desarrollo en la Jefatura de la División y otro bajo resguardo del desarrollador de sistemas de información.

Documentación de los desarrollos

» Documentar todas y cada una de las etapas del desarrollo de sistemas.
» Registrar las modificaciones que se realicen a los sistemas de forma inmediata a su

ejecución indicando usuario o departamento solicitante, modificación realizada y fecha de ejecución.
» Documentar los desarrollos de sistemas de información indicando el objetivo, tablas involucradas, subrutinas y fecha de actualización en cada bloque de código.
» La documentación de los desarrollos de sistemas permanecerá resguardada por el Secretario Académico de la DEP-FE.

Programas fuente

» Mantener una copia de los programas fuente de los desarrollos concluidos en el Centro de Cómputo.
» Mantener una copia de los programas fuente de los desarrollos en proceso en el Centro de Cómputo

Mantenimiento de los Sistemas de Información

» El mantenimiento a los sistemas de información deberá ser documentado indicando motivo de solicitud y fecha de implantación.
» Las modificaciones a los sistemas deberán ser probadas antes de implantarse en los ambientes de operación.
» La modificación o sustitución de código en el servidor deberá hacerse por el responsable del desarrollo de sistemas de información.
» Toda modificación o sustitución de código deberá realizarse en horarios no laborales o de baja demanda de los sistemas.

Diseño de Interfaz

» Se debe crear un diseño institucional para los sistemas de información y todos los reportes que de ellos se generen.
» Se debe crear y emplear una hoja de estilo para los Sistemas de Información de la DEP-FE.
» Registrar en la hoja de estilo cualquier modificación que sea realizada indicando usuario o departamento solicitante, objetivo, y fecha de ejecución.

Interactividad de las aplicaciones

» Implementar validaciones de datos de entrada, en especial para los caracteres -- > ; | .. / \ ‘ = y @.
» Implementar el manejo de eventos a fin de minimizar el número de datos proporcionados por el usuario.
» Desactivar el uso de los botones del ratón dentro de los sistemas de información.

Persistencia de Usuarios

» Emplear sesiones de usuario.
» Cerrar sesiones inactivas por más de quince minutos.

Políticas para la Seguridad en el servidor web

Configuración del servidor web
» Se debe modificar la configuración por default para que no se muestre la versión del servidor web. » Se debe modificar la cuenta de correo electrónico por default para evitar la potencial recepción de spam. » Se debe desactivar la opción de indexación de archivos y establecer un directorio público que sí sea indexado. » Se debe ocultar la versión del servidor, para evitar su reconocimiento. » Se debe personalizar el manejo de errores para que se no proporcione información particular del servidor. » Se deben inhabilitar los puertos que no sean utilizados por los sistemas de información. » Mantener una copia autorizada del contenido del sitio Web en otro host y/o en el área destinada para ello. » Inspeccionar los logs de transacciones así como actividades inusuales en el servidor, documentando los casos de intrusión. » En caso de falla de la línea, dar de baja a todos los usuarios que se encuentren conectados en ese momento.

Configuración del Módulo PHP
» Se debe activar el modo seguro para PHP. » Se debe deshabilitar el que se muestre la versión de php en los headers del servidor. » Se debe deshabilitar el desplegado de errores no graves de PHP. » Modificar la clave de acceso proporcionada para las conexiones al servidor cuando haya un cambio de personal: desarrollador, administrador, responsable del Centro de Cómputo.

Configuración de los servicios proporcionados
» Se debe evitar el uso de ftp público, restringiendo su uso sólo a personal autorizado. » Se debe configurar el servicio ssh para uso de protocolo seguro. » Se debe configurar el iptables para que sólo permite acceso a los puertos habilitados.

Políticas para la Seguridad en el Servidor de Base de Datos

Configuración del servidor
» Utilizar un usuario distinto al creado por default como administrador del RDBMS » Redireccionar las salidas, tanto estándar como de error hacia un archivo de log. » Modificar los permisos de acceso por default indicando qué usuario se puede conectar de manera local y cuáles de manera remota. » Cifrar el canal de comunicación entre el servidor y las conexiones remotas mediante SSL.

Políticas para la Seguridad en la Base de Datos

Diseño
» El Sistema Manejador de Bases de Datos (DBMS) que se utilice debe tener soporte para la creación y el manejo de índices, así como para manejar la integridad referencial. » Se debe realizar un buen análisis de requerimientos para implementar índices, llaves primarias y llaves foráneas en las tablas de la base de datos. » Se debe evitar en lo posible el almacenamiento de imágenes dentro de la base de datos. » Se debe utilizar en menor medida los tipos de datos texto e imagen por su complejidad en el procesamiento de información.

Acceso y procesamiento de la información
» Se debe utilizar sentencias SQL para el acceso a la información. » Cada sentencia SQL debe utilizar alias de los campos. » Se debe evitar realizar operaciones sobre tipos de datos de texto cuando éstos existan. » Las sentencias SQL deben acceder a los datos de manera secuencial a fin de minimizar el tiempo de acceso a los mismos.

Acceso a la base de datos
» El acceso a la base de datos se debe realizar mediante un clave de acceso y contraseña considerando también los roles de usuario. » Se debe mantener registro de los usuarios que acceden a la base de datos, fecha e ip de acceso. » Se debe registrar duración de sesión de cada usuario. » Se debe registrar el número de intentos fallidos por usuario. » Se deben generar estadísticas de entrada-salida para cada usuario.

Modificación al contenido de la Base de Datos
» Se debe registrar qué usuario realiza la inserción o modificación de registros de la base de datos de cada sistema de información. » Se debe realizar una validación a los datos modificados mediante scripts en el lado de los clientes.

Criptografía
» El algoritmo criptográfico a utilizar en la protección de la información es el MD5. » Las claves de acceso deben ser encriptadas con este algoritmo. » La información sensible en la base de datos también debe ser encriptada con este algoritmo.

Políticas para los Respaldos

Respaldos
» Concientizar al personal que los respaldos son de la información, no de las aplicaciones. » Se debe generar un respaldo de la configuración del servidor cada vez que se realice una modificación al mismo. » Se debe asegurar que el respaldo funcione de manera correcta. » Se debe almacenar un respaldo en el área de los servidores y otro en el Centro de Cómputo.

Auditorías

Auditoría a la base de Datos
» Se debe auditar el log de accesos a la base de datos de manera semanal. » Se deben realizar auditorías a la base de datos en periodos mensuales y trimestrales. » Se debe inhabilitar la clave de usuario que no haya sido usada en los últimos seis meses. » Se debe documentar los resultados de las auditorías, en particular aquellas donde se presenten problemas de consistencia de datos.

Auditoría a los Equipos de Cómputo
» La jefatura de la División de Estudios de Posgrado se reserva el derecho de vigilar e inspeccionar los equipos de cómputo en cualquier momento. » Estas inspecciones pueden llevarse a cabo con o sin el consentimiento y la presencia de los empleados involucrados. » Las inspecciones deben llevarse a cabo sólo después de haber obtenido la aprobación de los departamentos de personal y jurídico de la entidad académica.

5.3. Beneficios

Los beneficios que se observan en el corto plazo de la implementación del Sistema de Gestión de Seguridad de la Información es la concientización por parte de los usuarios de la necesidad de utilizar mecanismos de protección de la información, así como tener un mayor cuidado en el registro y manejo de la misma.

También se evidencia el riesgo que se corre al permitir que casi cualquier persona tenga acceso a las diversas áreas que integran a la DEP-FE, por lo que con esta Política de Seguridad de la Información se tendrá un mayor control y mejor registro sobre los accesos a las instalaciones físicas.

Otro beneficio, y tal vez uno de los mayores, es la documentación de los procesos críticos. Esto es de gran importancia ya que para cualquier eventualidad se contará con el soporte documental que indique la forma en que se restaurará el servicio interrumpido y así la restauración no dependerá totalmente de una persona específica, sino del proceso en sí mismo.

Los beneficios a largo plazo básicamente se enfocan al ordenamiento de las actividades operativas y a la reducción en los tiempos de respuesta para actividades cotidianas o excepcionales.

Finalmente, mediante el SGSI y la PSI se tendrá mayor confianza por parte de los usuarios en que los procesos que están realizando generan información que es almacenada y procesada de manera correcta y segura.

CONCLUSIONES

La seguridad de la información ha cobrado gran importancia en los últimos años, en especial porque casi todas las organizaciones han automatizado el proceso y almacenamiento de su información.

Esta seguridad en los sistemas de información debe ser vista a tres grandes niveles: seguridad interna, seguridad externa y seguridad de interfase. La seguridad externa se ocupa de la protección contra intrusos y desastres; la seguridad de la interfase con el usuario se encarga de establecer la identidad del usuario antes de permitir el acceso a los sistemas, y la seguridad interna se encarga de asegurar una operación confiable y sin problemas que garantice la integridad de los datos.

Estos niveles de seguridad son distintos para cada organización, ya que cada una requerirá un nivel de seguridad específico debido a que sus necesidades definen lo que para esa entidad significa seguridad.

Para implementar un nivel específico de seguridad es importante apoyarse en estándares, ya que el uso de éstos brinda mayor confianza debido a que cualquier especialista puede entenderlo, y no se está limitado al uso del producto de un fabricante particular; es por ello que se eligió el estándar internacional ISO/IEC 17799 cuyo objetivo es mejorar la eficiencia de la seguridad de la información mediante la implementación de una serie de controles asociados a las tecnologías de la información y a la infraestructura de comunicaciones, la cual proporciona las siguientes ventajas:

- Aumento de la seguridad efectiva de los sistemas de información
- Correcta planificación y gestión de la seguridad
- Garantías de continuidad del negocio
- Mejora continua a través del proceso de auditoría interna
- Incremento en los niveles de confianza
- Aumento del valor comercial y mejora de imagen de la organización
- Auditorías de seguridad más precisas y fiables

Este estándar sirvió de apoyo para desarrollar un Sistema de Gestión de Seguridad de la Información, cuya implementación es bastante compleja y requiere de un alto grado de compromiso, ya que al involucrar a todos los empleados de la organización implica el manejo de todas sus necesidades, así como del análisis de comportamientos y malas prácticas por parte de ellos o de externos.

Uno de los graves problemas que subsiste en la implementación de cualquier control de seguridad es la renuencia de los usuarios finales a acatar las políticas de seguridad, sobre todo en lo referente a la navegación por Internet y al manejo de correos electrónicos. Es por esto que se hace evidente la concientización de los usuarios respecto a las implicaciones de los problemas de seguridad, lo cual puede prevenir y disminuir el impacto de los incidentes cuando éstos ocurran.

Cabe aclarar que para mantener un nivel de seguridad específico se debe mantener actualizado el SGSI, ya que cubre aspectos relacionados con la política, la estructura organizacional, los procedimientos, los procesos y los recursos necesarios para la gestión de la seguridad de la información que a su vez contempla todas las áreas organizacionales de cualquier entidad, pues se cubren aspectos organizacionales, lógicos, y físicos, los cuales pueden estar en constante cambio.

Es importante destacar que no existe un control de seguridad único, sino que se deben combinar diversas tecnologías y herramientas utilizadas tanto en la protección como en ataques a los sistemas de información, para que con ello las organizaciones cuenten con diversas capas de seguridad y así poder detectar el problema en algunos de estos puntos antes de que llegue a la información crucial. Estas actualizaciones deben ser dadas a conocer a todo el personal involucrado, para que así realmente sean atendidas y respetadas.

Ahora bien, considerando que las causas de incidentes de seguridad informática pueden tener diversas fuentes (incluyendo la inexperiencia, el mal uso de las aplicaciones, los empleados disgustados y accidentes de mantenimiento), cualquier infraestructura de información debe contar, al menos, con las siguientes herramientas de seguridad:

- *Software antivirus*. Debe tenerse un mantenimiento adecuado para garantizar la protección de los quipos.
- *Infraestructura de red segura*. Deben considerarse conmutadores, switches y ruteadores que permitan una seguridad mínima a través de filtrado de paquetes y servicios de identificación y autenticación, así como una conectividad segura implementando a su vez la seguridad perimetral.
- *Hardware y software dedicados a la seguridad de la red*. En este caso se puede hablar de firewalls, tanto institucionales como personales.
- *Servicios de identidad*. Servicios que permiten la identificación de usuarios y las operaciones que realizan sobre la red. Estos servicios deben incluir contraseñas, certificados digitales y claves de autenticación digital.
- *Encriptamiento*. Mecanismos que garantizan que la información no pueda ser interceptada o leída por elementos no autorizados.
- *Administración de la seguridad*. Mecanismos mediante los cuales se conserva la interrelación entre los elementos mencionados a fin de mantener un nivel mínimo de seguridad para el sistema en cuestión.

Con los mecanismos de seguridad y la Política de Seguridad de la Información implementados podemos decir que se ha avanzado en la protección de la información generada, almacenada, transmitida y procesada de manera cotidiana en la División de Estudios de Posgrado de la Facultad de Economía.

LISTADO DE ACRÓNIMOS

ACK	Acknowledge. Confirmación de recepción
ARP	Address Resolution Protocol. Protocolo de resolución de direcciones
ARPA	Advanced Research Projects Agency
BS	British Standard. Estándar Británico
BS7799	Estándar británico para el manejo de la seguridad informática
BCP	Business Continuity Planning
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CCITSE	Common Criteria for Information Technology Security. Criterios Comunes para Seguridad de Tecnologías de la Información
CERT	Computer Emergency Response Team
CESG	Communications-Electronics Security Group
CIFE	Centro de Informática de la Facultad de Economía
CSR	Certificate Sign Request. Solicitud de firma de certificado
CSRF	Cross-Site Request Forgery
CSS	Cascade Style Sheets. Hojas de estilo
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DBMS	Data Base Manageent System. Sistema de Gestión o Administración de Base de Datos
DEP-FE	División de Estudios de Posgrado de la Facultad de Economía
DIDS	Distributed IDS
DMZ	DeMilitarized Zone. Red perimetral de una organización
DNS	Domain Name System. Conjunto de protocolos y servicios que permiten a los usuarios nombres de dominio en lugar de direcciones numéricas IP
DoS	Denial Of Service. Negación de un Servicio que normalmente está disponible
DOS	Sistema Operativo MS-DOS
DRP	Disaster Recovery Plan. Plan de Recuperación de Desastres
DSL	Digital Subscriber Line
EAL	Equipment Assurance Level. Nivel de garantía del equipo
ECMA	European Computer Manufacturing Association
EULA	End User License Agreement.
FC-ITS	Federal Criteria for Information Technology Security
HIDS	Host IDS

HTTP	HiperText Transfer Protocol. Protocolo de Transferencia de HiperTexto
ICMP	Internet Control Messaging Protocol
ID	Identificador
IDS	Intrusion Detection System. Sistema Detector de Intrusos
IEC	IT Evaluation Criteria. Criterios de Evaluación para las Tecnologías de la Información.
IP	Internet Protocol
IPS	Intrusion Prevention System. Sistema de Prevención de Intrusos
IRC	Internet Relay Chat. Protocolo de comunicación en tiempo real basado en texto
ISO	International Organization for Standarization. Organización Internacional para la Estandarización
IT	Tecnologías de la Información (TI). Término que comprende todas las formas de tecnología empleadas para crear, almacenar, intercambiar y usar información en sus formas variadas (datos de negocios, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia)
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
ITU	Internacional Telecomunication Unit. Unión Internacional de Telecomunicaciones
JTC	Joint Technical Comittee. Comité Técnico Conjunto
LAN	Local Area Network. Red de Área Local
MAC	Media Access Control
MD5	Message Digest, MD. Algoritmo de encriptamiento de 128 bits
MITRE	Organización privada sin fines de lucro que proporciona servicios técnicos y de ingeniería para el gobierno federal de los Estados Unidos de América. Una de sus áreas de desarrollo e investigación es la ingeniería de sistemas, tecnología de la información, conceptos operacionales y modernización de la empresa
NCSC	National Computer Security Center
NIDS	Network IDS
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCTAVE	Operational Critical Threat, Asset and Vulnerability Evaluation. Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo; permite evaluar las vulnerabilidades y amenazas que existen sobre los activos y operaciones críticas de una organización
PDA	Personal Digital Assistant. Asistente Digital Personal
PDCA	Plan – Do – Check – Act. Modelo de gestión de la seguridad de la información

PS	Política de Seguridad
PSI	Política de Seguridad de la Información
P2P	Peer-to-Peer
RAS	Rapad Access Server. Servidor de Acceso Rápido
RDSI	Red Digital de Servicios Integrados
RFC	Request for Comments. Solicitud Internet para Cometarios
RRN	Red Rusa de Negocios
RSA	Sistema criptográfico con clave pública llamado así por sus inventores: Rivest, Shamir y Adleman
SGSI	Sistema de Gestión de Seguridad de la Información
SIDEP-FE	Sistema de Información de la División de Estudios de Posgrado de la Facultad de Economía
SNMP	Simple Network Management Protocol. Protocolo Simple de Administración de Red
SMTP	Protocolo de Correo Electrónico
SPM	Specific Policy Management
SQL	Structured Query Language. Lenguaje Estructurado de Consultas
SSH	Secure Shell
SSL	Secure Socket Layer. Servicio de seguridad básico para protocolos de nivel superior, en particular HTTP
SYN	Paquete de establecimiento de conexión
TCP	Transmisión Control Protocol
TCP	Transmisión Control Protocol
TCP/IP	Transmisión Control Protocol / Internet Protocol
TCSEC	Trusted Computer Security Criteria, or Orange Book
TOE	Target Of Evalluation. Parte del producto o sistema que es objeto de evaluación
TOS	Time of Service
TTL	Time To Live
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	World Area Network. Red de Área Mundial
XSS	Cross-Site Scripting

GLOSARIO DE TÉRMINOS

Activo. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Adware. Advertising Supported software (Programa Apoyado con Propaganda). Son programas creados para mostrar propaganda.

Amenaza. Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Cualquier cosa que puede interferir con el funcionamiento adecuado de una computadora personal o causar la divulgación no autorizada de información almacenada en una computadora o sistema de información.

Análisis de riego. Evaluación de amenazas y vulnerabilidades de la información y su impacto en el procesamiento de la información así como su probabilidad de ocurrencia.

Ataque. Evento, exitoso o no, que atenta contra el buen funcionamiento del sistema.

Ataque Activo. Se nombra así a un ataque que implica algún tipo de modificación en el flujo de datos, a los propios datos o la creación de un falso flujo de datos.

Ataque Pasivo. Se nombra así a un ataque en el que el atacante no altera la información; únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

Autenticación. (Griego: αυθεντικός = verdadero o genuino, de ' los authentes' = el autor). Proceso mediante el cual algo o alguien es quien dice ser. En redes de equipos públicos y privados la autenticación se lleva a cabo a través de contraseñas de inicio de sesión

Back-Up. Son copias de datos, programas o información utilizadas como respaldo en caso de emergencia.

Backdoors. También conocidos como puertas traseras, son código inmerso en un programa que permite, a quien las conoce, saltarse los métodos usuales de autenticación para realizar ciertas tareas.

Base de Datos. Conjunto de datos organizados entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan.

Botnet. Colección de software robot o bots que se ejecutan de manera autónoma y que infectan a otros sitios.

BS7799. Estándar británico para el manejo de la seguridad informática.

Caballo de Troya. Es un programa al parecer inofensivo pero realmente lleva código imperceptible que se encarga de hacer daño.

CAPTCHA. (Completely Automated Public Turing test to tell Computers and Humans Apart). Sistema que se implementó como medida de seguridad para verificar que verdaderamente se trata de un ser humano el que intenta iniciar una sesión en un sitio de Internet.

CCITSE (Common Criteria for Information Technology Security). Criterios Comunes para Seguridad de Tecnologías de la Información.

Código malicioso. Cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas para robar, destruir o alterar la información.

Confidencialidad. Cualidad de la información por la cual sólo las personas autorizadas de un mensaje pueden leerlo

Contingencia. Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para una operación normal

Contraseña. Cadena de caracteres que el usuario escribe para verificar su identidad en una red o PC local.

Control de acceso. Mecanismo mediante el cual se definen derechos y privilegios sobre la utilización de recursos para un objeto o persona auténtica.

Controles. Son los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización. Indican una meta que debe ser alcanzada y lo que debe hacerse para lograr la protección de los activos.

Cookie. Una cookie (pronunciado ['ku.ki]; literalmente galleta) es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser recuperada posteriormente por el servidor que las creó en conexiones subsecuentes.

Cracker. Es aquel individuo que se especializa en saltar las protecciones anti-copia de software, de ahí el nombre crack para definir los programas que eliminan las restricciones en las versiones de demostración de software comercial.
También se asocia el término hacker a aquellas personas que poseen elevados conocimientos de seguridad informática para irrumpir en un sistema de cómputo ajeno para utilizarlo sin autorización.

Criptoanálisis. Se refiere a la ruptura o derrota de la criptografía, es decir, es el proceso que sin tener la autorización correspondiente intenta descubrir el texto o la clave.

Criptografía. Uso de códigos para proteger información por medio de una clave para que sólo el receptor específico pueda leerla. La criptografía es utilizada para permitir la autenticación y el no repudio, además de ayudar a preservar la confidencialidad y la integridad de los datos

Cross-Site Scripting (XSS). Vulnerabilidad que radica en la incorrecta validación de datos de entrada usados por una aplicación. No se limita a sitios web, ya que también se puede presentar en aplicaciones locales.
Mediante esta vulnerabilidad se puede ejecutar código VBScript o Java Script en el contenido de un sitio web.

Cross-Site Request Forgery (CSRF - Falsificación de petición en sitios cruzados). Tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio confía.
Esta vulnerabilidad también es conocida como XSRF, enlace hostil, ataque a un click, cabalgamiento de sesión o ataque automático.

CSR (Certificate Sign Request). Solicitud de firma de certificado.

Datos. Unidad mínima de información. Hechos y cifras que al ser procesados constituyen la información.

DBMS (Data Base Manageent System). Sistema de Gestión o Administración de Base de Datos. Proporciona las siguientes características: seguridad e integridad de los datos, provee lenguajes de consulta, provee una manera de introducir y editar datos de forma interactiva y, básicamente, existe independencia de los datos

Desastre. Cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el proceso normal de una empresa.

Disponibilidad. Estado de la información en le que los usuarios autorizados tienen acceso a ella cuando lo requieran.

DOS (Denial Of Service). Ataque que consiste en privar a una máquina de un recurso o un servicio del que normalmente dispone.

DNS (Domain Name System). Conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en lugar de tener que recordar direcciones IP numéricas.

DMZ (Demilitarized Zone). En seguridad informática una Zona DesMilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet; su objetivo es que las conexiones desde la red interna y la externa a la DMZ estén permitidas mientras que las conexiones desde la DMZ sólo se permitan a la red externa aislando de esta manera la red interna.

DRP (Disaster Recovery Plan). Plan de Recuperación de Desastres; es el conjunto de procedimientos alternativos a la operación normal de una organización, cuyo objetivo es definir las pautas necesarias para una adecuada recuperación de la información, en caso de ser necesario, y permitir su funcionamiento cuando alguna de sus divisiones deje de funcionar debido a algún incidente ya sea interno o ajeno a la organización mediante una metodología definida para recuperar el procesamiento de recursos críticos.

EAL (Equipment Assurance Level). Nivel de garantía del equipo.

Encriptamiento. El encriptamiento es una forma efectiva de disminuir los riesgos en el uso de tecnología. Implica la codificación de información para que sólo el emisor y el receptor la puedan leer.

EULA (End User License Agreement). Es una licencia para la cual el uso de un producto sólo está permitido para un único usuario (el comprador), utilizando éste en una forma determinada y de conformidad con unas condiciones convenidas.
La licencia, que puede ser gratuita u onerosa, especifica los derechos (de uso, modificación o redistribución) concedidos a la persona autorizada y sus límites. Además, puede señalar el plazo de duración, el territorio de aplicación y todas las demás cláusulas que el titular del derecho de autor establezca.

Evaluación del riesgo. Comparación de los resultados de un análisis del riesgo con los criterios estándares del riesgo u otros criterios de decisión.

Exploit. Programa para explorar agujeros y, aprovechando la debilidad, falla o error en el sistema, ingresar en él.

Exposición. Denominación que otorga el MITRE cuando un ataque se realiza por una debilidad o una política de seguridad inapropiadaza.

Firewall. Dispositivo que funciona como filtro entre redes, permitiendo o denegando las transmisiones de una red a la otra. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Gateway. En Telecomunicaciones es una computadora o nodo de la red que permite o controla el acceso de/hacia otra computadora o red con estándares, arquitecturas y protocolos diferentes. Su función principal traducir los datos al lenguaje o protocolo que utiliza la conexión de entrada.

Gusano. Programa que se propaga a sí mismo por una red, normalmente a través de correo electrónico, TCP/IP o dispositivo de almacenamiento externo. Se reproduce a sí mismo a medida que se ejecuta.

Freeware. El término inglés freeware define un tipo de software de computadora que se distribuye sin costo y por tiempo ilimitado. En ocasiones se incluye el código fuente, pero no es lo usual.

Hacker. Hacker es el neologismo utilizado para referirse a un experto en alguna o varias ramas técnicas relacionadas con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etcétera.
El término Hacker trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Hacking. Intrusión informática no deseada o acceso ilegítimo a los sistemas de información.

Hijacking. Técnica que consiste en alterar la información contenida en el paquetes. Es decir, modificar los datos en sí.

Hoax (virus falso). Son mensajes con falsas advertencias de virus, o de cualquier otro tipo de alerta, de cadena o de algún tipo de denuncia distribuida mediante el correo electrónico. Los objetivos de estas alertas son causar alarma, pérdida de tiempo, robo de direcciones de correo y/o saturación de los servidores; su común denominador, es pedirle los distribuya "a la mayor cantidad posible de conocidos".

Impacto. Consecuencia de la materialización de una amenaza.

Ingeniería Social. Consecuencia de la materialización de una amenaza.

Integridad. Cualidad de un objeto si no ha sido modificado, ampliado o recortado. Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema.
El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

IP. Internet Protocol.

IP hijacking. Se produce cuando un atacante consigue interceptar una sesión ya establecida.

IP spoofing. Ataque en el que un sistema asume la dirección IP de otro para suplantarlo.

ISO (International Organization for Standarization). Organización Internacional para la Estandarización.

IT. Tecnología de la Información.

ITSEC. Information Technology Security Evaluation Criteria.

Keylogger. Un keylogger (registrador de teclas) es una herramienta de diagnóstico utilizada en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet.

Lammer. Persona con pocos conocimientos técnicos e informáticos que consigue e intercambia herramientas no desarrolladas por ellos mismos que les permiten atacar sistemas ajenos. No investigan, sólo ejecutan aplicaciones sin conocer bien sus efectos, pero cuyas consecuencias pueden ser muy dañinas.

Malware (abreviatura de Malicious software, también llamado badware). Término que engloba a todo tipo de programas o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento del mismo.

Manejo del riesgo. Proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar sistemas de la información, por un costo aceptable.

MD5 (Message Digest, MD). Algoritmo de encriptamiento de 128 bits.

Mecanismo de seguridad. Conjunto de elementos o procesos que implementan un servicio de seguridad, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.

MITRE. Organización privada sin fines de lucro que proporciona servicios técnicos y de ingeniería para el gobierno federal de los Estados Unidos de América. Una de sus áreas de desarrollo e investigación es la ingeniería de sistemas, tecnología de la información, conceptos operacionales y modernización de la empresa

Modelo de Seguridad. Presentación formal de una política de seguridad ejecutada por el sistema.

No repudio. El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Es un servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

OpenSource (Código abierto). Es el término con el que se conoce al software distribuido y desarrollado libremente. Fue utilizado por primera vez en 1998 por algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original en inglés del software libre (free software).

Pishing. Término informático mediante el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria

Plan de contingencia. Estrategia planificada con una serie de procedimientos que faciliten u orienten en la generación de una solución alternativa para sustituir de manera rápida los servicios proporcionados por una organización ante la eventualidad de todo lo que se pueda paralizar, ya sea de forma parcial o total.

Privacidad. Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundida o transmitida a otros.

Política de Seguridad. Conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad.

Proxy. En el contexto de las redes informáticas, el término proxy hace referencia a un programa o dispositivo que realiza una verificación de accesos y privilegios. La finalidad más habitual es la del servidor proxy que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Ramsomware. Técnica de secuestro de archivos que impide el acceso del usuario a sus propios documentos hasta que pague cierta cantidad de dinero. Este troyano busca en la computadora de la víctima archivos de tipo Word o Excel y los "zipea" con un password, envía notificación al usuario y los libera una vez realizado el pago indicado.

Riesgo. Posibilidad de que se produzca un impacto determinado sobre un activo, en un dominio o en toda la organización.

Rootkit. Son pequeños programas con rutinas encriptadas que se instalan en forma oculta en los sistemas de los usuarios de equipos persoonales y servidores para evitar ser detectados por los antivirus, software de seguridad y utilitarios de administración de los sistemas.
Son un conjunto de herramientas de software usados por intrusos que acceden ilícitamente a un sistema operativo. Estas herramientas sirven para ocultar procesos y archivos en su ejecución, frecuentemente con fines maliciosos, tales como inicios de sesión (logins), procesos, archivos, creación o modificación de llaves de registro, etc..; pueden interceptar datos contenidos en un sistema, conexiones de red y hasta digitaciones del teclado (Keyloggers).

Seguridad. Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer; todo está bien.
Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

Seguridad de la información. Conjunto de procesos, procedimientos, tareas y actividades implementados conjuntamente apoyados en elementos de cómputo y telecomunicaciones que permiten controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos (información, equipos, etc.) ubicados en un sitio específico, durante su estadía en un medio de almacenamiento o durante su transmisión, en sus aspectos de integridad, disponibilidad, confidencialidad y autenticidad

Seguridad Informática. Nombre genérico dado a una colección de herramientas diseñadas para proteger datos y detener a los perpetradores

Servicio de seguridad. Es aquel que está dirigido a evitar ataques de seguridad desde un aspecto muy particular buscando la seguridad de un sistema de información y el flujo de la información de una organización. Los principales servicios de seguridad son: control de acceso, confidencialidad, integridad, disponibilidad y no repudio.

Shareware. Programas realizados generalmente por programadores independientes, aficionados o empresas pequeñas que quieren dar a conocer su trabajo permitiendo que su programa sea utilizado gratuitamente por todo aquel que desee probarlo.
Estos programas se pueden instalar y usar, e incluso distribuir libremente (sin modificarlo), sin pago alguno; lo que el autor le pedirá, en caso de que emplee su programa satisfactoriamente durante mucho tiempo, es que le envíe una cantidad simbólica de dinero para sufragar el esfuerzo de dedicar tiempo a la realización de programas. Las empresas que eligen este método para dar a conocer sus programas no suelen habilitar todas las funciones

de sus programas en la versión shareware, por lo que le enviarán la versión incompleta del programa.

Sniffer. Programa o dispositivo que analiza el tráfico de datos que pasa por un punto de la red en la que está instalado.

Spam (correo masivo). Práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas web.

Spoofing. Técnica utilizada para enviar paquetes con la dirección de origen falseada.

Spyware. Son pequeños programas que se instalan en nuestro sistema con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red.
Trabajan en modo background (segundo plano) de modo que el usuario no se percata de su existencia hasta que empieza a generarse un comportamiento anormal en el equipo.

SSL (Secure Socket Layer). Servicio de seguridad básico para protocolos de nivel superior, en particular HTTP.

TCP/IP. Transmisión Control Protocol / Internet Protocol

TCSEC. Trusted Computer Security Criteria, u Orange Book.

TI (Tecnologías de la Información). Término que comprende todas las formas de tecnología empleadas para crear, almacenar, intercambiar y usar información en sus formas variadas (datos de negocios, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquellas que aún no se han concebido). Es un término conveniente para incluir tanto a la telefonía como a la tecnología de cómputo en una misma palabra.

TOE (Target Of Evalluation). Parte del producto o sistema que es objeto de evaluación.

Tripwire. Tripwire es un programa de computadora Open Source consistente en una herramienta de seguridad e integridad de datos. Tripwire es útil para monitorizar y alertar de cambios específicos de archivos en un rango de sistemas.

Vulnerabilidad. Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

Wardriving. Técnica que utilizan los hackers y que está bastante difundida. Piratas, equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos de acceso inalámbricos. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc...
Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un punto de acceso a redes inalámbricas. Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

Warspamming. Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

Web spoofing. Técnica mediante la cual se crea una copia falsa de un sitio web. Los accesos a ésta son encaminados hacia el equipo del atacante, lo cual le permite observar todas y cada una de las actividades de la víctima, incluyendo las entradas de contraseñas o números de cuenta que introduzca.

Worms. Serie de videojuegos del género de estrategia militar por turnos. En estos juegos se enfrentan dos o más jugadores que controlan uno o varios personajes durante cierto tiempo con el objetivo de eliminar a los personajes de los adversarios.

BIBLIOGRAFÍA

[1] *Seguridad Informática. ¿Qué, por qué y para qué?* Revista RED, noviembre 2002.

[2] *Seguridad en redes de computadores*. Diplomado en Telemática y Negocios por Internet - Escuela Colombiana de ingeniería. 1999.

[3] FUSTER SABATER Amparo, DE LA GUIA MARTÍNEZ Dolores, HERNÁNDEZ ENCINAS Luis, MONTOYA VITINI Fausto, MUÑOZ MASQUE Jaime. *Técnicas Criptográficas de protección de Datos*. Segunda Edición Actualizada. México, 2001.

[4] KARANJIT S. Siyan, Ph. D., HARE Chris. *Firewalls y la Seguridad en Internet*. Segunda Edición. Prentice-Hall Hispanoamericana S.A. 1997

[5] LÓPEZ BARRIENTOS María Jaquelina y QUEZADA REYES Cintia, *Fundamentos de seguridad informática*, Facultad de Ingeniería, UNAM. 2006, 223 pp.

[6] U.S. Department of Defense. *Trusted Computer System Evaluation Criteria (TCSEC).* Diciembre 1985

[7] Office for Official Publications of the European Communities. *Information Technology Security Evaluation Criteria Version 1.2* (ITSEC), Junio 1991.
Disponible en http://www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF

[8] Canadian System Security Centre. *Canadian Trusted Computer Product Evaluation Criteria.* Enero 1993

[9] The National Institute of Standards and Technology. *Federal Criteria for Information Technology Security* - FC, Enero 1993

[10] International Organization for Standardization. Information technology | Security techniques | Evaluation criteria for IT security. *ISO/IEC 15408*. Diciembre 1999

[11] Instituto Argentino de Normalización. *Esquema 1 de Norma IRAM-ISO IEC 17799. Tecnología de la Información. Código de prácticas para la administración de seguridad de la información*. Argentina, 2002.

[12] MAGAÑA CISNEROS Adrián. *Diplomado de Seguridad en Redes y Telecomunicaciones*. DECFI-UNAM. México, 2007.

[13] National Institute of Standards and Technology. Technology Administration. US Department of Commerce. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12

[14] Instituto Nacional de Estadística e Informática. *Guía práctica para el desarrollo de Planes de Contingencia de Sistemas de Información*. Lima, 2001.

[15] SILES PELÁEZ Raúl. *Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados*. Primera edición. 2002

[16] CHESWICK William R., BELLOVIN Steven M. (Contributor). *Firewalls and Internet Security: Repelling the Wily Hacker*. Segunda Edición. Addison-Wesley. 2000

[17] RFC 2554. SMTP Service Extension for Authentication

[18] NÚÑEZ SANDOVAL Alejandro. *Taller de Desarrollo de Políticas de Seguridad. Seminario Admin-UNAM. "Mecanismos básicos de seguridad para redes de cómputo"*. DGSCA–UNAM, 2005.

[19] RFC 1244 Site Security Handbook, Julio. 1991
http://tools.ietf.org/html/rfc1244

[20] Spafford, Gene. *Manual de Seguridad en Redes*. ARCERT Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública. Argentina. 2000.

[21] Universidad Nacional de Colombia. Vicerrectoría General. Dirección General de Informática y Comunicaciones. *Guía para elaboración de Políticas de seguridad*. 2003

[22] MURUGESAN San, Deshpande Yogesh (Eds.), *Web Engineering: Managing Diversity and Complexity of Web Application Development*. 2001

[23] NÚÑEZ SANDOVAL Alejandro. *Implantación de Bases de Datos Seguras en PostgreSQL V 8.2.6*. Seguridad CERT-DGSCA-UNAM. México, 2008.

[24] SALIBA, Rima y SAINT-GERMAIN René. *Una herramienta para implantar la norma BS 7799 / ISO 17799*. 2008
http://www.callio.com

[25] ANLEY, Chris. *Advanced SQL Injection In SQL Server Applications*. NGSSoftware Insight Security Research (NISR). 2002.

REFERENCIAS ELECTRÓNICAS

[W1] *¿Qué es la seguridad informática?* Santiago C. Claudia. Centro de Estudios de Telemática. Escuela colombiana de Ingeniería Julio Garavito. 2005
http://www.citel.oas.org/newsletter/2005/septiembre/seguridad_e.asp

[W2] *Nuevas tendencias del malware*. Fuentes Serrano Luis Fernando. Revista Enterate – UNAM, 2005
http://www.enterate.unam.mx/Articulos/2005/agosto/malware.htm

[W3] *The Internet Word*. MORRIS Robert Jr.. 1988.
http://www.zyvex.com/nanotech/worm.html

[W4] *Net Dialogue*
http://netdialogue.org

[W5] TCSEC
https://www.ccn-cert.cni.es/publico/2008/401/es/t/tcsec.htm

[W6]OCTAVE
http://www.kwell.net/ioctave.htm

[W7] Algunas afirmaciones erróneas comunes acerca de la seguridad
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

[W8] Ingeniería Social
http://www.rompecadenas.com.ar/ingsocial.htm

[W9] El Top 20 de las vulnerabilidades de Windows y Linux
http://www.vivalinux.com.ar/articulos/top-20-vulnerabilidades

[W10] Boletín de seguridad 2007 de Kaspersky Lab. La evolución de las amenazas en 2007
http://www.viruslist.com/sp/analysis?pubid=207270972

[W11] Planes de contingencia
http://hispasecurity.com

[W12] Arquitectura de Seguridad de la Información en la Empresa
http://enterprisearchitecture.nih.gov/About/Approach/Framework.htm

[W13] Consideraciones de diseño para aplicaciones Web
http://www.informatizate.net/articulos/consideraciones_de_seguridad_en_el_diseno_de_aplicaciones_web_16082004.html

ANEXO 1

CUESTIONARIO DE LA NORMA UNE-ISO/IEC 17799

1 - POLÍTICA DE SEGURIDAD

Pregunta 1.1

¿Existe publicado un documento de políticas, aprobado por la dirección, publicado y comunicado de forma apropiada a todos los empleados?

o Sí o Parcialmente ⊗No o No aplicable o Asumir

Justificación:

Se han dado algunos casos de política en cómputo pero hay renuencia por parte de algunos profesores

Pregunta 1.2

¿Es la política publicada revisada regularmente y sobre todo en caso de cambios influyentes?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

No es publicada pero sí revisada

2 – ASPECTOS ORGANIZACIONALES DE LA SEGURIDAD

Pregunta 2.1

¿Hay un comité directivo que asegure que hay una directriz clara y un soporte visible desde la alta dirección en todas las iniciativas de seguridad?¿El comité de dirección promueve la seguridad por medio de un compromiso apropiado y una dotación adecuada de recursos?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

No se ha convocado a un Comité

Pregunta 2.2

En aquellas organizaciones de gran tamaño, ¿Está la implementación de los controles de seguridad coordinados a través de un grupo multifuncional de representantes de la dirección provenientes de todas las partes relevantes de la organización?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 2.3

¿Han sido claramente definidas las responsabilides para la protección de activos concretos y la realización de procesos específicos de seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

No hay en ninguna área

Pregunta 2.4
¿Existe un proceso de gestión de autorización activo para nuevas infraestructuras de tratamiento de la información?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 2.5
¿Hay un consejero especializado en la seguridad de la información buscado dentro o fuera de la organización para coordinar los conocimientos y asistir al a toma de decisiones en asuntos de seguridad?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 2.6
¿Mantiene su organización contactos apropiados con autoridades responsables de hacer cumplir la ley, cuerpos regulatorios, proveedores de servicios de información y operadores de telecomunicación?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 2.7
¿Es revisada de forma independiente la implementación de la política de seguridad de la información en su organización?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Está asignada con otras actividades inherentes de cómputo

Pregunta 2.8
¿Han sido calculados los riesgos asociados con el acceso a las infraestructuras organizativas de tratamiento de la información por terceras partes, y han sido implementados los controles apropiados de seguridad?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 2.9
¿Especifican los contratos con terceras partes que suponen acceder a las infraestructuras de tratamiento de la información de su organización, de todos los requerimientos y condiciones necesarias de seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 2.10

¿Están claramente definidos y acordados entre todas las partes los requerimientos de seguridad a la gestión externa y el control de todos o algunos de sus sistemas de información, redes y/o puestos de trabajo de usuarios, y expresados en el contrato de externalización?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

3 - CLASIFICACIÓN Y CONTROL DE ACTIVOS

Pregunta 3.1

¿Existe un inventario de todos los activos importantes asociados con cada sistema de información, esquematizado y mantenido?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Sólo inventario del equipo de cómputo

Pregunta 3.2

¿Hay controles de clasificación y protección adecuados a las necesidades de negocio para compartir o restringir información, y los impactos sobre el negocio asociados a dichas necesidades?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Existen sistemas heterogéneos y diferentes demandas de los usuarios que no permiten implementar un control general

Pregunta 3.3

¿Existen procedimientos implantados para etiquetar y manejar información de acuerdo con el esquema de clasificación adoptado por su organización?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

4 - SEGURIDAD ASOCIADA AL PERSONAL

Pregunta 4.1

¿La definición de puestos de trabajo incluye los roles y responsabilidades de seguridad tal como se hayan definido en la política de seguridad de la información de la organización?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 4.2

¿Se realizan verificaciones sobre los empleados fijos, contratatistas y personal temporal en la fase de selección del mismo?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 4.3

¿Firman los empleados acuerdos de confidencialidad como parte de sus términos y condiciones iniciales de empleo?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 4.4

¿Están las responsabilidades para la seguridad de la información de los empleados expresados en sus términos y condiciones e empleo?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 4.5

¿Los empleados de la organización, y cuando sean relevantes, usuarios de terceras partes, reciben una formación y puesta al día apropiada en procedimientos y políticas organizativas?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 4.6

¿Son informados por canales de gestión adecuados los incidentes de seguridad tan pronto como se hayan detectado?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Son informados de manera distinta; no existe un procedimiento establecido

Pregunta 4.7
¿Se ha requerido a los usuarios informar de cualquier vulnerabilidad o amenaza de seguridad sobre servicios o sistemas de la cual se tenga sospecha?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:
En algunos casos se ha brindado información verbal

Pregunta 4.8
¿Se siguen todos los procedimientos para informar del mal funcionamiento del software?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:
Se ha informado sobre el mal uso que le dan a un software determinado

Pregunta 4.9
¿Se han establecido mecanismos para permitir cuantificar y monitorizar el volumen y coste para la organización de los incidentes de seguridad y malos funcionamientos de la infraestructura de tratamiento de la información?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 4.10
¿Las violaciones de las políticas y procedimientos de seguridad realizadas por los empleados son tratadas con procesos disciplinarios?
o Sí o Parcialmente ⊗o No o No aplicable o Asumir
Justificación:
Se considera irrelevante

5 - SEGURIDAD FÍSICA Y DEL ENTORNO

Pregunta 5.1
¿Se utilizan perímetros de seguridad para proteger las áreas que contienen infraestructuras de tratamiento de la información?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 5.2
¿Se encuentran las áreas de seguridad protegidas por controles de entrada apropiados para asegurar que sólo acceda personal autorizado?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 5.3

¿Han sido creadas áreas seguras para proteger oficinas, despachos e infraestructuras que tengan requerimientos especiales de seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 5.4

¿Existen controles y directrices adicionales para trabajar en áreas seguras que mejoren la seguridad provista por controles físicos?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 5.5

¿Se han desarrollado áreas controladas de carga y descarga, preferentemente aisladas de las infraestructuras de tratamiento de la información para evitar accesos no autorizados?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 5.6

¿Está el equipamiento protegido para reducir los riesgos de amenazas y peligros ambientales y accesos no autorizados?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:

Son protecciones normales como puertas con doble chapa, pero aún así no hay control de accesos no autorizados

Pregunta 5.7

¿Está protegido el equipamiento de fallos de energía y otras anomalías eléctricas?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:

Sólo en áreas seleccionadas; el porcentaje es muy bajo

Pregunta 5.8
¿Se encuentran protegidos de interceptaciones o daños los cables eléctricos y de telecomunicaciones que soporten servicios de información o transporten datos?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
En algunas áreas la protección de cables de red es nula. En algunas áreas las conexiones eléctricas se encuentran en muy mal estado

Pregunta 5.9
¿Está el equipamiento correctamente mantenido para permitir que no pierda su integridad y disponibilidad?
o Sí ⊗ Parcialmente ⊗ No o No aplicable o Asumir
Justificación:
Se cuenta con campañas de mantenimiento a los equipos de cómputo, tanto en actualización de vacunas como limpieza de componentes en los periodos intersemestrales

Pregunta 5.10
¿Hay implantado un proceso de gestión de autorizaciones relativo al uso del equipamiento para el tratamiento de la información fuera de las premisas de la organización?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Existe la posibilidad de acceso a las instalaciones en días y horario no laboral con la consecuente responsabilidad de no hacer mal uso de las instalaciones

Pregunta 5.11
¿Es borrada la información de los equipos que se vayan a eliminiar o a reutilizar?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:
Aunque son pocos los usuarios que lo solicitan, los equipos que se dan de baja o reasignan son formateados y cargados con nuevo software

Pregunta 5.12
¿Opera la organización con una clara política de "mesa despejada y pantalla bloqueada" para proteger la información de pérdida, daños o uso no autorizado?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 5.13
¿Cuando se tiene que suprimir equipamiento que tiene software e información que pertenece a la organización, se requiere la autorización de la dirección?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:
En ocasiones el usuario final llega a eliminar la información

6 - GESTIÓN DE COMUNICACIONES Y OPERACIONES

Pregunta 6.1

¿Están los procedimientos operativos identificados, documentados y mantenidos en la política de seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.2

¿Están controlados los cambios a las infraestructuras de tratamiento de la información y los sistemas?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Los cambios se realizan conforme se van requiriendo

Pregunta 6.3

¿Han sido establecidos responsabilidades y procedimientos de gestión de incidentes para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad y la recopilación de datos, registros de logs y rastros de auditoría relativos a los mismos?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.4

¿Han sido segregadas las funciones y áreas de responsabilidad con objeto de reducir las oportunidades de realizar modificaciones no autorizadas o usar inadecuadamente la información o los servicios?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.5

¿Se encuentran separadas las infraestructuras de desarrollo y pruebas de los sistemas de explotación y hay reglas definidas y documentadas que ordenan la migración del software desde desarrollo a producción?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

No se cuenta con la posibilidad de mantener en espejo los servidores de aplicación a fin de mantener una maqueta de pruebas

Pregunta 6.6
¿Previamente al uso de infraestructuras de servicios de gestión externas, han sido identificados apropiadamente los riesgos y se han acordado controles de seguridad con el contratista, y han sido incorporados al contrato?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.7
¿Son monitorizadas las demandas de capacidad y se realizan requerimientos de capacidad futura para permitir que siempre esté disponible la potencia adecuada de cálculo y almacenamiento?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.8
¿Existe un criterio de aceptación establecido para nuevos sistemas de información, subidas de versión, y plan de pruebas previamente a su aceptación?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:
En equipos de cómputo se realizan pruebas para evaluar una actualización de versión de software comercial y sugerir al usuario qué versión utilizar. Respecto a los sistemas desarrollados, existen lagunas respecto al nivel mínimo de aceptación

Pregunta 6.9
¿Existen controles de prevención y detección para protegerse contra software malicioso y se han implantado procedimientos apropiados de concientización a los usuarios?

⊗ Sí o Parcialmente o No o No aplicable o Asumir

Justificación:
Todos los equipos personales cuentan con software antiespía

Pregunta 6.10
¿Existen copias de backup de información y software esencial para el negocio y son restauradas para testear su recuperabilidad regularmente?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:
Se ha sugerido a los usuarios la adquisición de discos duros para realizar respaldos pero ha sido casi nula la respuesta

Pregunta 6.11
¿El personal de operaciones mantienen un log de sus actividades y están estos logs sujetos a chequeos regulares e independientes?

o Sí o Parcialmente o No o No aplicable ⊗ Asumir

Justificación:

Pregunta 6.12
¿Se informan los errores y se toman las acciones correctivas correspondientes?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Se plantea al usuario el error en el que puede incurrir y se sugieren acciones correctivas, sin embargo en ocasiones no se registra la contingencia y por lo tanto no existe seguimiento a la misma

Pregunta 6.13
¿Se ha implementado un rango de controles para alcanzar y mantener la seguridad en las redes?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 6.14
¿Existe procedimientos de gestión de los soportes informáticos removibles como cintas, discos, cassettes e informes impresos?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:
Si es para que se almacene información, sí. El servicio es solicitado a través de un formato.

Pregunta 6.15
¿Han sido establecidos procedimientos para deshacerse de forma segura de los soportes?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo el área de la jefatura cuenta con triturado de papel

Pregunta 6.16
¿Han sido establecidos procedimientos para el manejo y el almacenamiento de la información que los proteja de una divulgación no autorizada o un mal uso?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 6.17
¿Está protegida la documentación de los sistemas del acceso no autorizado?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 6.18
¿Han sido establecidos acuerdos para el intercambio (electrónico y manual) de información y software entre organizaciones?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 6.19
¿Están los soportes en tránsito protegidos para su uso no autorizado, inadecuado o corrupción?
o Sí o Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 6.20
¿Está protegido el comercio electrónico contra actividades fraudulentas, disputas contractuales y divulgación o modificación de la información?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 6.21
¿Ha sido desarrollada una política para el correcto uso del correo electrónico y han sido implementados controles para vigilar los riesgos de seguridad inherentes al mismo?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Se trata de que el personal de áreas administrativas use correos institucionales

Pregunta 6.22
¿Han sido preparadas e implementadas políticas para controlar los riesgos de negocio y seguridad asociados con la ofimática?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 6.23
¿Hay un proceso formal de autorización aplicado antes de que se haya hecho públicamente disponible la información y su integridad ha sido protegida para prevenir modificaciones no autorizadas?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 6.24
¿Han sido implementadas políticas, procedimientos y controles para proteger el intercambio de la información a través de las infraestructuras de comunicación de voz, fax y video?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

7 - CONTROL DE ACCESOS

Pregunta 7.1
¿Han sido definidos y documentados los requerimientos de negocio para el control de acceso, y ha sido éste acceso restringido de acuerdo a lo que se haya definido en la política de control de acceso?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:
Sólo para el acceso a las salas de trabajo (préstamo de equipo de cómputo) se solicita una identificación

Pregunta 7.2
¿Han sido implantados procedimientos para el registro y des-registro de usuarios para garantizar el acceso a toda la información, sistemas y servicios?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:
Existe un registro de entrada y salida a las salas de trabajo

Pregunta 7.3
¿Está restringida y controlada la designación y utilización de privilegios?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:
En equipos de servicio está restringido el acceso.
En los sistemas de información se encuentran controlados y se mantiene registro a los mismos

Pregunta 7.4
¿Está controlada la asignación de contraseñas a través de un proceso formal de gestión?

o Sí ⊗ Parcialmente o No o No aplicable o Asumir

Justificación:
En equipos de uso administrativo donde se han presentado anomalías y mal uso del software

Pregunta 7.5
¿Son revisados a intervalos regulares los derechos de acceso de los usuarios utilizando procesos formales?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.6
¿Se requiere a los usuarios que sigan unas buenas prácticas de seguridad en la selección y uso de contraseñas?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Se les sugiere el uso de contraseñas que no sean obvias

Pregunta 7.7
¿Se ha requerido a los usuarios que se aseguren que todo el equipamiento desatendido tenga la protección apropiada?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 7.8
¿Se permite a los usuarios que sólo tengan acceso directo a aquellos servicios que estén específicamente autorizados para usar?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:
En los equipos que tienen restricciones

Pregunta 7.9
¿Está controlado el camino desde el terminal de usuario al servicio informático?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 7.10
¿Está sujeto el acceso remoto de usuarios a chequeos de autenticación?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
En los sistemas desarrollados se ha implementado estos controles

Pregunta 7.11
¿Son autenticadas las conexiones a sistemas informáticos remotos?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 7.12
¿Está controlado el acceso a puertos de diagnóstico con la seguridad necesaria?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 7.13
¿Existen controles implantados en redes que segregen grupos de servicios de información, usuarios y sistemas de información?
o Sí o Parcialmente o No o No aplicable ⊗Asumir
Justificación:

Pregunta 7.14
¿La capacidad de conexión de usuarios en redes compartidas está restringida de acuerdo a la política de control de acceso?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 7.15
¿Tienen las redes compartidas controles de routing o encaminamiento de forma que el flujo de información no viole la política de control de acceso a aplicaciones de negocio?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.16
¿Ha sido obtenida una clara y documentada descripción de los atributos de seguridad de todos los servicios de redes que se proveen?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.17
¿Son identificados automáticamente los terminales al autenticar conexiones a localizaciones específicas y a equipos portátiles?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.18
¿El acceso a los servicios de información se realiza vía un proceso de registro seguro?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.19
¿Se les ha provisto a los usuarios con un identificador único (user ID) para su exclusivo uso personal de forma que puedan seguirse las actividades de los individuos, y ha sido seleccionada una técnica de autenticación adecuada para comprobar la identidad asociada a cada usuario?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 7.20
¿Hay implantado un sistema de gestión de contraseñas que provea de una eficiente e interactiva facilidad para la creación de contraseñas de calidad?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 7.21
¿Está controlado y restringido el uso de programas de utilidad del sistema?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo en equipos de uso administrativo

Pregunta 7.22
¿Hay alarmas anti-coacción provistas para usuarios que podrían ser objetivo de coacción?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 7.23
¿Están implantados procedimientos y mecanismos para asegurarse de que terminales inactivos en localizaciones de alto riesgo o sirviendo a sistemas de alto riesgo, se apagarán después de un periodo definido de tiempo de inactividad para prevenir el acceso a personas no autorizadas?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.24
¿Hay restricciones sobre las horas de conexión a aplicaciones de alto riesgo para proveerlas de seguridad adicional?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.25
¿Esta restringido el acceso a la información y a funciones de los sistemas de aplicación en concordancia con la política de control de accesos?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 7.26
¿Los sistemas sensibles tienen entornos informáticos aislados y dedicados?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Área de servidores

Pregunta 7.27
¿Están produciendo los logs de auditoría registros por excepción y otros eventos relevantes de seguridad, y son todos ellos retenidos por un periodo de tiempo suficiente para poder realizar en el futuro investigaciones y monitorización del control de acceso?
o Sí o Parcialmente ⊗o No o No aplicable o Asumir
Justificación:

Pregunta 7.28
¿Hay procedimientos establecidos para monitorizar el uso de infraestructuras de tratamiento de la información y son el resultado de actividades de monitorización revisadas regularmente?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Mediante losgs de accesos a los sistemas de información

Pregunta 7.29
¿Están todos los relojes de los ordenadores sincronizados para un registro adecuado de eventos y acciones?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 7.30
¿Existe una política formal implantada y controles apropiados para protegerse del riesgo de trabajar con infraestructuras informáticas móviles, especialmente en entornos no protegidos?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 7.31
¿Hay implantadas políticas, procedimientos y estándares para autorizar y controlar actividades de teletrabajo?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Únicamente en las salas de videoconferencia

8 - DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Pregunta 8.1
¿Los requerimientos de negocio de nuevos sistemas o mejoras a los existentes, especifican requerimientos de controles?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 8.2
¿Son validados los datos de entrada a los sistemas de aplicación para asegurarse que son correctos y apropiados?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.3
¿Han sido incorporados chequeos de validación dentro de los sistemas para detectar la corrupción de datos?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.4
¿Ha sido implantado un sistema de autenticación de mensajes donde hay un requerimiento de seguridad para proteger la integridad del contenido del mensaje?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 8.5
¿Se valida los datos de salida de los sistemas de aplicación para asegurar que el procedimiento de almacenamiento de la información es correcto y adecuado a las circunstancias?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.6
¿Hay una política sobre el uso de controles criptográficos para la protección de la información?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 8.7
¿Se aplica la encriptación para proteger la confidencialidad de información crítica o sensible?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
En algunos casos en el uso de contraseñas

Pregunta 8.8
¿Se ha aplicado la firma digital para proteger la autenticidad e integridad de la información electrónica?
o Sí ⊗Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo para el registro de calificaciones en el sistema de información de la DGAE

Pregunta 8.9
¿Se están usando servicios de no repudio para resolver disputas acerca de la ocurrencia o no ocurrencia de eventos o acciones?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 8.10
¿Se está utilizando un sistema de gestión de claves para soportar el uso de técnicas criptográficas, basado sobre un grupo de estándares, procedimientos y métodos?
o Sí o Parcialmente o No o No aplicable ⊗ Asumir
Justificación:

Pregunta 8.11
¿Hay procedimientos implantados para controlar la implementación de software o de sistemas operativos?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
En algunos casos, por ejemplo las restricciones para instalar software

Pregunta 8.12
¿Están controlados y protegidos los datos de prueba?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.13
¿Se mantiene un estricto control sobre el acceso a las librerías de programas fuente?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.14
¿Existen procedimientos formales de control de cambios para la implementación de los mismos?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 8.15
¿Son revisados y probados los sistemas de aplicación cuando ocurren los cambios?
⊗ Sí o Parcialmente o No o No aplicable o Asumir
Justificación:

Pregunta 8.16
¿Están las modificaciones a los paquetes de software no recomendadas y cualquier cambio esencial estrictamente controlado?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo en los equipos asignados a áreas administrativas

Pregunta 8.17
¿Se controla y chequea cualquier uso o modificación del software para protegerlo contra conversiones no autorizadas y códigos troyanos?.
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
En equipos de áreas administrativas

Pregunta 8.18
¿Hay controles aplicados a asegurar el desarrollo externalizado de software?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

9 - ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Pregunta 9.1
¿Hay implantado un proceso de gestión para desarrollar y mantener la continuidad de negocio por toda la organización?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 9.2
¿Hay un plan estratégico activo, basado en al valoración de riesgos, detallando el enfoque general de la continuidad de negocio?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 9.3
¿Se han desarrollado planes para mantener o restaurar operaciones de negocio de forma periódica siguiendo a la interrupción de, o un fallo de, procesos críticos de negocio?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo en el caso de un servidor, existe uno de respaldo

Pregunta 9.4
¿Se mantiene un marco único de planes de continuidad de negocio que asegure que todos los planes son consistentes e identifique prioridades para pruebas y mantenimiento?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 9.5
¿Son probados regularmente los planes de continuidad de negocio y son mantenidos por revisiones regulares de forma que siempre estén al día y sean efectivos?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

10 - CUMPLIMIENTO DE LA NORMATIVIDAD

Pregunta 10.1
¿Están todos los requerimientos relevantes, regulatorios, estatutarios y contractuales explícitamente definidos y documentados para cada sistema de información.
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo existen normatividades para el uso de equipos del Centro de Cómputo

Pregunta 10.2
¿Se han implementado procedimientos apropiados para asegurar el cumplimiento de restricciones legales sobre el uso del material respecto a los derechos de propiedad intelectual, y todos los otros propietarios de software?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 10.3
¿Son protegidos los registros importantes para la organización para evitar su pérdida, destrucción y falsificación?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo en áreas de servidores

Pregunta 10.4
¿Se han aplicado controles para proteger la información personal de acuerdo con la legislación relevante?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 10.5
¿Existe autorización por parte de la dirección para el uso de infraestructuras de tratamiento de la información y se han aplicado controles para prevenir el uso inadecuado de dichas infraestructuras?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
No hay vigilanvia

Pregunta 10.6
¿Existen controles implantados para asegurar el cumplimiento con acuerdos nacionales, leyes, regulaciones u otros instrumentos para controlar el acceso a, o el uso de controles criptográficos?
o Sí o Parcialmente ⊗ No o No aplicable o Asumir
Justificación:

Pregunta 10.7
¿Cuando en las acciones contra una persona u organización intervenga la ley, civil o criminal, se realiza la recolección de evidencias de acuerdo a las reglas legales o según un código estándar de prácticas para la producción de evidencias admisibles en tribunales de justicia?
o Sí ⊗ Parcialmente o No o No aplicable o Asumir
Justificación:
Sólo en algunos casos excepcionales de robo

Pregunta 10.8
¿La dirección toma acciones para asegurarse de que todos los procedimientos de seguridad son realizados correctamente? adicionalmente, ¿Están todas las áreas dentro de la organización sujetas a una revisión general para asegurar el cumplimiento de las políticas y estándares de seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 10.9
¿Se chequean regularmente los sistemas de información para verificar su conformidad con los estándares de implementación de la seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 10.10
¿Son cuidadosamente planeadas las auditorías de los sistemas de explotación y están orientados a minimizar el riesgo de perturbaciones a los procesos de negocio?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

Pregunta 10.11
¿Está protegido el acceso a las herramientas de auditoría para prevenir posibles usos inadecuados o el compromiso de su seguridad?

o Sí o Parcialmente ⊗ No o No aplicable o Asumir

Justificación:

ANEXO 2

SELECCIÓN DE CONTROLES

A continuación se presentan los controles seleccionados así como su detalle de análisis y propuesta de solución para la División de Estudios de Posgrado de la Facultad de Economía (DEP-FE).

GESTIÓN DE OPERACIONES Y COMUNICACIONES

Control a evaluar	**CONTROL DE CAMBIOS EN LOS SERVIDORES DE APLICACIÓN**	
Política de Seguridad	Se mantendrá un registro de los cambios a la configuración y al hardware que se realice a los servidores de procesamiento de información de la DEP-FE	
Evaluación del riego	El control inadecuado de estos cambios puede generar fallas en la seguridad y en el desempeño de los sistemas de información	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Se deben implementar responsabilidades y procedimientos formales para garantizar un control satisfactorio de todos los cambios en el hardware, el software o los procedimientos de operación de los servidores de aplicaciones • Cuando se cambian los programas, se debe tener una bitácora donde se registren los cambios realizados a fin de reestablecer el ambiente original de los servidores de aplicación • Cuando exista un cambio de área física de los servidores, se debe documentar la interrupción de aplicaciones, cerrado de las mismas, apagado del equipo, reconexión, reinicialización y activación de procesos en el reestablecimiento de los servicios • Cada servidor debe contar con una batería en buen estado a fin de responder de manera activa en caso de fallas de energía o de voltaje
Solución	*Tareas y actividades específicas a realizar*	• Realizar el registro de cambio de hardware en el inventario de activos de la DEP-FE. La aplicación de gestión de inventario se encuentra desarrollada en *Visual FoxPro* • Realizar el cambio de responsable del equipo en caso de sustituir el servidor de aplicaciones • Para el caso de migración a un nuevo servidor, realizar pruebas de instalación, configuración y desempeño de las aplicaciones antes de liberarlo para su uso cotidiano. • Generar una bitácora por servidor y registrar los cambios significativos en el proceso de migración • Notificar a los usuarios pertinentes del nuevo cambio y llevar a cabo las configuraciones necesarias en cada equipo Terminal. Cada vez que exista una reinstalación o recompilación de las aplicaciones en los servidores, ésta debe estar documentada de tal manera que se incluyan las fallas o errores, una descripción de las mismas y la solución que se les dio.

Control a evaluar	**MANEJO DE INCIDENTES**	
Política de Seguridad	Se deben establecer responsabilidades y procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad	
Evaluación del riego	La falta de registro de manejo de incidentes evita su seguimiento y cumplimiento de la seguridad si existen o reinciden fallos en la misma y son desatendidos	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Dar seguimiento a los reportes de negación del servicio registrando las causas del mismo • Realizar un registro de pérdida de servicio delimitando el área afectada
Solución	*Tareas y actividades específicas a realizar*	• Registrar y analizar la causa del incidente a fin de evitar su repetición • Analizar la frecuencia de pérdida de servicio relaciona con la segmentación de la red Registrar en una bitácora la causa de la pérdida de servicio generando estadísticas del problema • Notificar a los encargados de servidores de la DEP y obtener su retroalimentación en lo referente a la solución de problemas

Control a evaluar	**PLANIFICACIÓN Y APROBACIÓN DE SISTEMAS**	
Política de Seguridad	Realizar proyecciones a futuro en lo referente a capacidad del equipo a fin de reducir el riesgo de saturación del sistema garantizando la disponibilidad de procesamiento y almacenamiento adecuados.	
Evaluación del riego	Los sistemas de información pueden llegar a colapsarse en caso de no contar con infraestructura suficiente para soportar el funcionamiento del sistema	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Desempeño y requerimientos de capacidad de las computadoras, ya que esto impacta en el presupuesto de la organización
Solución	*Tareas y actividades específicas a realizar*	• Realizar más de una propuesta de mainframe considerando procesadores, almacenamiento principal, almacenamiento de archivos, impresoras y otros medios de salida ("output"), así como los sistemas de comunicaciones (actuales y futuros) • Capacitación al personal en el uso de los nuevos sistemas a fin de evitar el mal uso de los nuevos sistemas • Realizar pruebas exhaustivas para evitar cualquier conflicto con el servidor de aplicaciones y con propia infraestructura de la DEP-FE • Establecer métricas o parámetros de verificación

Control a evaluar	**PROTECCIÓN CONTRA SOFTWARE MALICIOSO**	
Política de Seguridad	Todos los equipos deben contar con software antivirus como protección local así como con una configuración adecuada del firewall personal	
Evaluación del riego	El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso como pueden ser virus informáticos, *worms* de red, *troyanos* y bombas lógicas	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Campañas antivirus semestrales • Actualizaciones periódicas de vacunas antivirus • Configuración periódica de firewalls personales • Configuración del equipo para evitar la instalación de software no autorizado
Solución	*Tareas y actividades específicas a realizar*	• Concientización a los usuarios sobre el peligro del software no autorizado o malicioso • Implementación de Firewalls institucionales a fin de realizar un filtrado de tráfico • Verificación contra virus de nuevas aplicaciones, software a instalar o dispositivos que se conecten al equipo de los usuarios • Verificación de software malicioso en archivos adjuntos a correo electrónico y/o descargas de Internet • Actualización de los programas antivirus, firewall personal, anti-spyware y anti-spam

Control a evaluar	**RESGUARDO DE LA INFORMACIÓN**	
Política de Seguridad	Se debe realizar de manera periódica copias de resguardo de la información así como de la configuración de los servidores de aplicaciones críticas para la DEP-FE. Esta copia de seguridad debe ser probada a fin de determinar su correcto funcionamiento garantizando con ello su confiabilidad	
Evaluación del riego	El no contar con procesos de respaldo implica la pérdida de activos (tiempo, dinero y esfuerzo) al duplicar las labores debido a la pérdida de la información al ocurrir un desastre o falla de los dispositivos	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Documentación de los procesos de respaldo de información de los servidores de aplicación crítica de la DEP-FE • Documentación de los procesos de recuperación de información de acuerdo con los respaldos de información realizados • Se deben tener al menos tres periodos de respaldo de información (semanal, mensual, bimestral, semestral, etc.)
Solución	*Tareas y actividades específicas a realizar*	• Generar la documentación correspondiente a los procesos de respaldo y de recuperación de información mediante los respaldos realizados • Capacitarse a nuevo personal en la generación y recuperación de respaldos de información de los servidores a fin de tener el personal capacitado en caso de requerirse • Los procesos de levantamiento de servidores, así como apagado de los mismos deberá permanecer resguardado por el responsable del Centro de Cómputo y por el propio administrador de servidores

Control a evaluar	**REGISTRO DE FALLAS**	
Política de Seguridad	Llevar un registro de fallas en el procesamiento de la información o los sistemas de comunicación	
Evaluación del riego	El no contar con un registro de fallas evita la realización de estudios de comportamiento de los sistemas de información y de la infraestructura de la red, minando con ello la posibilidad de realizar análisis de los mismos a fin de evitar futuras fallas.	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Correcto levantamiento de fallas en la infraestructura de la red • Garantizar que todas las fallas reportadas han sido resueltas de manera satisfactoria • Generación de esquemas técnicos de distribución de dispositivos en la infraestructura de red de la DEP-FE
Solución	*Tareas y actividades específicas a realizar*	• Generación de esquemas de red de la DEP-FE a fin de determinar los segmentos a los cuales corresponden los equipos de los usuarios • Seguimiento correcto al levantamiento de fallas verificando con el usuario final que la respuesta proporcionada sea correcta para el problema detectado

Control a evaluar	**SEGURIDAD DEL CORREO ELECTRÓNICO**	
Política de Seguridad	Se establecerán niveles de acceso a fin de bloquear el uso de estas aplicaciones en los equipos de empleados que no tengan necesidad de hacer uso de este servicio	
Evaluación del riego	El uso indiscriminado del correo electrónico genera pérdida de tiempo de los empleados de la DEP-FE y pone en riesgo a la organización al replicar correos que no siempre se verifica su origen.	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Los correos electrónicos sólo le son asignados a profesores, adjuntos, personal administrativo de confianza, y miembros de los órganos directivos • Bloquear el acceso al correo electrónico a aquellas personas que no tienen necesidad de utilizarlo para realizar sus labores • Eliminar de manera periódica el correo spam o sin utilidad (junk mail)
Solución	*Tareas y actividades específicas a realizar*	• Restringir la instalación de servicios de correo electrónico • Llevar un registro por equipo de los accesos a Internet o alguna otra aplicación no permitida al usuario

CONTROL DE ACCESOS

Esta sección tiene como objetivo evaluar los controles de acceso de los usuarios a cualquiera de los elementos conectados o de cualquier otro elemento vinculados con el tráfico de la red, a fin de señalar irregularidades que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información, así como las recomendaciones correspondientes para mejorar el servicio.

Para el caso de servidores y computadoras conectadas a la red no se tiene en cuenta ninguna restricción horaria para el uso de los recursos y sólo se considera una restricción física sobre servidores.

Control a evaluar	**REGISTRO DE USUARIOS**	
Política de Seguridad	Debe existir un procedimiento formal de registro y cierre de sesión de usuarios para otorgar acceso a todos los sistemas y servicios de información.	
Evaluación del riego	El no contar con un registro de accesos genera un hueco de seguridad muy grande ya que no hay forma de responsabilizar a los usuarios por mal uso, abuso, o modificación de la información.	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Utilizar identificadores de usuario de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones • Verificar que el usuario tiene autorización del gestor del sistema para hacer uso del mismo o tener acceso a la información • Verificar que el nivel de acceso otorgado es el adecuado en base a las funciones y ámbito de acción de cada usuario del Sistema • Mantener un registro formal de todas las personas autorizadas para utilizar el servicio, el cual contenga nombre, área de adscripción • Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o ya no laboran en la organización • Verificar periódicamente, y cancelar cuentas de usuarios e identificadores redundantes • Garantizar que los identificadores de usuario no se reasignen a otro usuario
	tareas y actividades específicas a realizar	• Se debe contar con bitácora de usuarios para tener el registro de alta, baja y/o modificación de usuarios • Se debe contar con un IDS a fin de contar con hardware que pueda ser programado y llevar el registro de acciones realizadas en los equipos conectados a la red

Control a evaluar	**SEGURIDAD DEL CORREO ELECTRÓNICO**	
Política de Seguridad	Se establecerán niveles de acceso a fin de bloquear el uso de estas aplicaciones en los equipos de empleados que no tengan necesidad de hacer uso de este servicio	
Evaluación del riego	El uso indiscriminado del correo electrónico genera pérdida de tiempo de los empleados de la DEP-FE y pone en riesgo a la organización al replicar correos que no siempre se verifica su origen.	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Bloquear el acceso al correo electrónico a aquellas personas que no tienen necesidad de accesarlo para realizar sus labores
Solución	*Tareas y actividades específicas a realizar*	• Restringir la instalación de servicios de correo electrónico • Llevar un registro por equipo de los accesos a Internet o alguna otra aplicación no permitida al usuario

Control a evaluar	**ADMINISTRACIÓN DE PRIVILEGIOS**	
Política de Seguridad	Se debe mantener un registro y control de la asignación de privilegios para los distintos sistemas de información con que cuenta la DEP-FE	
Evaluación del riego	El no contar con una correcta asignación de privilegios puede generar errores en los sistemas al ser utilizada la información por empleados no autorizados	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Debe evitarse el uso de la clave de root para cuestiones distintas a la administración o configuración • Eliminar usuarios predefinidos en sistemas operativos y bases de datos • Deben definirse los privilegios a los usuarios del sistema operativo en base su rol y actividades (administradores, desarrolladores, usuarios comunes) • Deben definirse privilegios a los usuarios de las bases de datos (administrador, usuarios, aplicaciones)
Solución	*Tareas y actividades específicas a realizar*	• Se ha definido la asignación de privilegios en base al rol de los usuarios. • Se evita el uso de root para cualquier tarea diferente a la administración o configuración

Control a evaluar	**ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO**	
Política de Seguridad	Se otorgarán contraseñas a los usuarios de los sistemas de información de la DEP-FE a fin de mantener un registro de sus actividades dentro de los mismos	
Evaluación del riego	El no contar con un registro de accesos y el seguimiento a las acciones realizadas dentro del sistema nos impide llevar un correcto seguimiento de los usuarios dentro de los sistemas de información de la DEP-FE	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Generación de contraseñas temporales • Registro de contraseñas con métodos de encriptamiento
Solución	*Tareas y actividades específicas a realizar*	• Generar declaraciones de confidencialidad de las contraseñas otorgadas a los usuario haciendo que las firme quien las reciba • Proporcionar una contraseña temporal a los nuevos usuarios por un periodo corto de tiempo hasta que ellos realicen el cambio de la misma. Estas contraseñas temporales sólo serán asignadas una vez identificado de manera fehaciente al usuario (se puede utilizar el sistema **CAPTCHA** - Completely Automated Public Turing test to tell Computers and Humans Apart) • Para la asignación de nuevas claves, NO deberá usarse mensajes sin protección (texto claro), ya que cualquier intruso podría interceptar el mensaje y hacer un mal uso del mismo. Para realizar una protección de claves, podemos usar la herramienta Paros, que además de funcionar como Proxy, Spider o Scanner de web nos permite codificar y decodificar en varios formados; su distribución es gratuita y se puede obtener en http://www.parosproxy.org • Se debe solicitar el acuse de recibo de la nueva clave • El registro de las contraseñas deberá estar protegido con algún método de encriptación. En este caso se ha utilizado MD5 ya que a la fecha no existe forma de vulnerarlo

Control a evaluar	**REVISIÓN DE DERECHOS DE ACCESO DE USUARIO**	
Política de Seguridad	Se debe implementar un plan de revisión de derechos de acceso de usuarios a fin de mantener actualizados los perfiles de los mismo considerando su movilidad dentro de la organización	
Evaluación del riego	El mantener cuentas con derechos de acceso sin modificación generan el conocimiento de la misma por personas no responsables de la misma con el consecuente riesgo de uso o mal uso de la información	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Generar procedimiento de revisión y modificación regular de derechos de acceso de los usuarios
Solución	*Tareas y actividades específicas a realizar*	• Revisar constantemente la asignación de claves de acceso y sus derechos a fin de eliminar aquellas que ya no se usan o se han divulgado • En caso de tener claves de acceso difundidas o pertenecientes a personal altamente riesgoso, eliminarlas y/o modificarlas en un periodo semanal. • Revisar los privilegios de usuario de manera regular (trimestralmente) a fin de mantener un correcto control de los mismos de acuerdo con los roles de usuarios

Control a evaluar	**USO DE CONTRASEÑAS**	
Política de Seguridad	Mantener un registro de contraseñas seguras validando cada cambio a realizar	
Evaluación del riego	El manejo incorrecto de las contraseñas puede generar problemas de derechos de acceso a los diversos sistemas de información de la DEP-FE	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Notificar a los usuarios de mantener sus contraseñas en secreto • Modificar las contraseñas y realizar la notificación correspondiente en caso de que existan indicios de compromiso de los sistemas de información
Solución	*Tareas y actividades específicas a realizar*	• Realizar una revisión física de las áreas de usuario a fin de determinar si existen contraseñas registradas en documentos de acceso fácil (papel, papelera, …) • Capacitar a los usuarios para que sepan cómo determinar una contraseña segura: longitud, no datos personales o laborales • Cambiar periódicamente las contraseñas de acceso evitando la reutilización de las mismas • Cambiar las contraseñas temporales en el primer log-on • Incluir contraseñas en los procesos de acceso a la BD • Modificar las rutas de acceso a los sistemas de información de manera periódica

Control a evaluar	**EQUIPOS DESATENDIDOS EN ÁREAS DE USUARIOS**	
Política de Seguridad	Los usuarios deben garantizar que los equipos desatendidos están protegidos adecuadamente	
Evaluación del riego	Todos los usuarios deben proteger por sí mismos la información con la que trabaja, en caso contrario, ésta puede ser mal usada por un tercero teniendo consecuencias que van desde sólo su conocimiento hasta la difusión de la misma	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Concientizar a los usuarios del riesgo de dejar desatendido un equipo de cómputo y de su responsabilidad sobre el mismo • Capacitar a los usuarios en el correcto cierre de sesión en los sistemas de información
Solución	*Tareas y actividades específicas a realizar*	• Modificar los accesos a los equipos de forma tal que SIEMPRE solicite una clave de acceso • Modificar la configuración de los equipos para que pasado un tiempo en que el equipo se encuentre desatendido se active el protector de pantalla y sólo se pueda desbloquear mediante clave de acceso • Implementar mecanismos de protección en los sistemas desarrollados a fin de que pasado un tiempo de inactividad se cierre la sesión inactiva • Mantener un registro de cierre de sesión de los usuarios a fin de notificar cuando éste no ocurra

Control a evaluar	**PROTECCIÓN DE LOS PUERTOS (PORTS) DE DIAGNOSTICO REMOTO**	
Política de Seguridad	Los puertos de los servidores de aplicación deberán estar cerrados a menos que exista un sistema de información que haga uso de él. En el A**nexo 3** se muestra un listado de puertos	
Evaluación del riego	El mantener abiertos puertos no utilizados genera una puerta de acceso a usuarios mal intencionados o no permitidos a los servidores de aplicación	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Deberá contarse con un procedimiento de conexión externa en caso de no poder acceder físicamente al área de servidores
Solución	*Tareas y actividades específicas a realizar*	• Cerrar los puertos que no son utilizados • Generar el procedimiento de acceso remoto a los servidores de aplicación • Limitar el acceso remoto a los puertos

Control a evaluar	**SUBNETEO DE REDES**	
Política de Seguridad	Definir subredes seguras dentro de la organización	
Evaluación del riego	El mantener todos los equipos de red conectados a un mismo nodo genera mayor tráfico en la red con la consecuente lentitud. De igual manera, se genera una administración deficiente de los recursos y de las aplicaciones utilizadas	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Los perímetros serán implementados a través de Gateway entre subredes que serán interconectadas a fin de controlar el acceso y flujo de información entre dominios • Implementación de Firewall para acceso a Internet
Solución	*Tareas y actividades específicas a realizar*	• Configurar el Gateway para realizar filtrado de tráfico entre dominios, así como bloqueo de acceso no autorizado

Control a evaluar	**RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN**	
Política de Seguridad	Sólo los responsables del desarrollo tendrán acceso directo a las Bases de Datos de las aplicaciones a fin de verificar el correcto funcionamiento de dichos sistemas	
Evaluación del riego	En caso d e que persona ajena al área de desarrollo tenga acceso a la información, puede corromper ésta, por lo que deberá mantenerse resguardada a través de claves de acceso y éstas serán modificadas conforme a los criterios de administración de contraseñas	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Definir los niveles de acceso para los diferentes usuarios de los sistemas de información • Definir un correcto control de acceso de los usuarios en base al rol de cada uno
Solución	*Tareas y actividades específicas a realizar*	• Generar un control de acceso de información mediante las políticas de seguridad y acceso a la misma • Revisar las salidas de los sistemas de información a fin de garantizar que sólo presenten la información requerida, ya sea mediante las vistas o mediante código HTML que pudiera ser analizado • Revisar que las salidas de información sólo lleguen a los equipos autorizados para tal fin dentro de la organización

Control a evaluar	**MONITOREO DE ACTIVIDADES DENTRO DE LA RED**	
Política de Seguridad	Se debe realizar el monitoreo de las actividades que realizan los usuarios dentro de la infraestructura de telecomunicaciones	
Evaluación del riego	El realizar acciones fuera de las permitidas compromete en un alto grado el nivel de confiabilidad que se tiene en las aplicaciones de la DEP-FE, por lo que se debe evitar el uso y abuso de la infraestructura para acciones no académicas	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Llevar un registro de las acciones realizadas por los usuarios de la red, poniendo mayor atención a: • acceso no autorizado, incluyendo detalles como: o ID de usuario; o Fecha y hora de eventos clave; o Tipos de eventos; o Archivos a los que se accede; o Utilitarios y programas utilizados • todas las operaciones con privilegio, como: o Utilización de cuenta de supervisor; o Inicio y cierre (start-up and stop) del sistema; o Conexión y desconexión de dispositivos I/O; • intentos de acceso no autorizado, como: o Intentos fallidos; o Violaciones de la política de accesos y notificaciones para "gateways" de red y "firewalls"; o Alertas de sistemas patentados para detención de intrusiones ; • alertas o fallas de sistema como: o excepciones del sistema de registro; o alarmas del sistema de administración de redes.
Solución	*Tareas y actividades específicas a realizar*	• Realizar un monitoreo de al menos tres meses y hacer un análisis de los resultados obtenidos • Generar una bitácora de eventos encontrados

DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Control a evaluar	**VALIDACIÓN DE DATOS DE ENTRADA**	
Política de Seguridad	Validar los datos de entrada a fin de asegurar su integridad	
Evaluación del riego	El ingreso de información distinta a la requerida corromperá la Base de Datos con la consecuente falta de integridad de la misma y pérdida	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Realizar una validación de los datos de entrada a fin de detectar alguno de los siguientes errores: o Valores fuera de rango o Caracteres inválidos en tipos de datos o Datos faltantes o incompletos o Control de datos inconsistentes
Solución	*Tareas y actividades específicas a realizar*	• Realizar la validación de datos relevantes tales como nombres, rfc's, número de cuenta, entidades académicas, entre otros. • Generar los programas correspondientes para responder a errores de validación • Evitar en lo posible el uso de JavaScript ya que puede proporcionar información referente al sitio de información • Evitar que el DBMS genere un mensaje de error, ya que con ello puede dar información referente a la estructura de la base de datos

Control a evaluar	**CONTROLES Y VERIFICACIONES**	
Política de Seguridad	Deben existir métodos de comprobación de la información que se registra	
Evaluación del riego	El no realizar controles y verificación de los datos genera inconsistencia en los mismo con la consecuente incongruencia en la información	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Realizar la definición de entidades de la BD • Generar procesos de integridad de datos de la BD • Verificar la secuencia lógica de los programas y aplicaciones de los sistemas de información
Solución	*Tareas y actividades específicas a realizar*	• Para cada nueva entidad, validar sus dependencias funcionales e implementar los controles para actualización y borrado de información en cascada • Verificar que la información registrada tenga una correspondencia de acuerdo al DER de los sistemas de información auditados

Control a evaluar	**CIFRADO DE LA INFORMACIÓN**	
Política de Seguridad	Toda información sensible y crítica deberá estar cifrada a fin de evitar su robo o mal uso de la misma.	
Evaluación del riego	El tener la información en texto plano facilitará a los intrusos la extracción de datos de los Sistemas de Información	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Identificar el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado, así como la longitud de las claves criptográficas a utilizar •
Solución	*Tareas y actividades específicas a realizar*	• Implementar mecanismos de cifrado en los datos sensibles en todas y cada una de las entidades de la DB de los Sistemas de Información • Generar código ejecutable que permita el encriptado de información que se transmite por la red. A la fecha uno de los métodos de cifrado seguro son el MD5 ya que no existe algoritmo de desencripción

Control a evaluar	**PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS**	
Política de Seguridad	La administración de claves criptográficas debe utilizarse siempre que se utilice alguna técnica criptográfica. Estas claves deben estar protegidas contra modificación o destrucción.	
Evaluación del riego	La pérdida de claves criptográficas compromete la confidencialidad, integridad y autenticidad de la información	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Definir el tipo de clave a utilizar: pública o privada • Generar una clave por cada sistemas de información con que se cuente • Determinar periodos de validez de las claves
Solución	*Tareas y actividades específicas a realizar*	• Proteger la clave • Generar y obtener certificados de clave pública para los sistemas de información • Revocar las claves cuando éstas se encuentren comprometidas o cuando un usuario se desvincula de la DEP-FE • Auditar las actividades realizadas por claves específicas • Generar certificados de claves públicas para el acceso y administración de los Sistemas de Información

Control a evaluar	**CONTROL DEL SOFTWARE OPERATIVO**	
Política de Seguridad	El software operativo deberá ser la última versión revisada y autorizada por el responsable del área cuyo sistema se está implementando	
Evaluación del riego	El mantener versiones no actualizadas de las aplicaciones puede llegar a generar inconsistencias en la información registrada, así como permitir la existencia de huecos de seguridad	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Generar el procedimiento de actualización de versiones ejecutables para los sistemas de información de la DEP-FE • Generar una bitácora de actualizaciones de sistemas operacionales
Solución	*Tareas y actividades específicas a realizar*	• Eliminar cualquier código fuente que se encuentre residente en el servidor de aplicaciones • En caso de contar con código interpretado, proteger los directorios correspondientes • El software operativo no debe ser publicado hasta que haya sido probado exhaustivamente evidenciando que cumple con los requerimientos del usuario • Realizar un respaldo de las versiones actuales de los Sistemas e Información como medida precautoria en caso de requerir restaurar el funcionamiento del sistema.

Control a evaluar	**CONTROL DE ACCESO A LAS BIBLIOTECAS DE PROGRAMA FUENTE**	
Política de Seguridad	E responsable del área de desarrollo deberá contar con respaldos diarios de programas fuente	
Evaluación del riego	El no contar con respaldos diarios propia la pérdida de seguimiento en el desarrollo de software El contar con los respaldos de código fuente garantiza la continuidad del desarrollo en caso de accidente o abandono por parte del programador	
Gestión del Riesgo	*Procesos y Procedimientos a implementar*	• Generar procedimiento de respaldo de programas fuente en servidores que no estén operando • Designar un bibliotecario de programas por cada aplicación
Solución	*Tareas y actividades específicas a realizar*	• Evitar el acceso incontrolado a los programas fuente • La actualización de versiones en el servidor de operación deberá ser llevada a cabo por el responsable de las mismas • Se debe llevar a cabo una bitácora de actualización de versiones

ANEXO 3

PROCEDIMIENTOS DEL PLAN DE CONTINGENCIAS

ÍNDICE

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.1 CONFIGURACION DEL SERVIDOR WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/4
01	01	2009	

OBJETIVOS

Realizar una configuración específica y especializada en el servidor web de la División de Estudios de Posgrado de la Facultad de Economía a fin de minimizar el riesgo de ataques y con ello asegurar la continuidad de la operación.

POLITICAS

1. Modificar la configuración por default para evitar vulnerabilidades conocidas para la última versión del sistema.

2. Mantener actualizada la versión del servidor web conforme surjan nuevas formas de ataque y solución a las mismas.

3. Deshabilitar los puertos de comunicación que no sean utilizados por los sistemas de información de la DEP-FE.

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.1 CONFIGURACION DEL SERVIDOR WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/4
01	01	2009	

DESCRIPCIÓN

INTERVENCION	ACTIVIDAD

ADMINISTRADOR DEL SERVIDOR APACHE	1. Editar el `httpd.conf`
	2. Ocultar la versión del servidor mediante `ServerTokens min`.
	3. Modificar la cuenta de correo por default de manera que sea referenciada de forma institucional `webadmin@sidepfe.unam.mx`.
	4. Modificar los valores de User y Group a uno determinado para el sitio, en este caso `sidepfe_admin` y `sidepfe_group`.
	5. Desactivar el keep-alive `KeepAalive Off`.
	6. Modificar las ligas simbólicas para evitar que algunos directorios sean expuestos; debe quedar solamente Options FollowSymLink.
	Esta opción debe estar acompañada por el directorio público que sí permite ligas simbólicas
	`<Directory "/var/www/html/public">`
	`Options FollowSymLinks Indexes`
	`Order allow,deny`
	`Allow from all`
	`</Directory>`
	7. Deshabilitar el mod_user una vez que se han implementados los virtual-host

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.1 CONFIGURACION DEL SERVIDOR WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	3/4
01	01	2009	

DESCRIPCIÓN

INTERVENCION	ACTIVIDAD

ADMINISTRADOR DEL SERVIDOR APACHE	9. Modificar el tipo de archivo a interpretar de modo que parezca que se tiene un servidor Microsoft-IIS `AddType application/x-httpd-php .asp`
	10. Configurar el CustomLog para almacenar todas las ocurrencias de posible ataque
	`CustomLog log/access_log combined`
	11. Ocultar información del servidor
	`ServerSignature off`
	12. Comentar el bloque de la sección del manual de apache
	`<Directory "/var/www/manual">`
	`. . .`
	`</Directory>`
	13. Personalizar los mensajes de error de manera que muestren la menor cantidad de información del servidor
	`ErrorDocument 400 /error/error.hrml`
	`ErrorDocument 401 /error/error.hrml`
	`ErrorDocument 403 /error/error.hrml`
	`ErrorDocument 405 /error/error.hrml`
	`ErrorDocument 406 /error/error.hrml`
	`ErrorDocument 407 /error/error.hrml`
	`ErrorDocument 410 /error/error.hrml`
	`ErrorDocument 412 /error/error.hrml`
	`ErrorDocument 414 /error/error.hrml`
	`ErrorDocument 500 /error/error.hrml`
	`ErrorDocument 501 /error/error.hrml`
	`ErrorDocument 502 /error/error.hrml`

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.1 CONFIGURACION DEL SERVIDOR WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	4/4
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD

ADMINISTRADOR DEL SERVIDOR APACHE	14. Habilitar el virtual host
	`NameVirtualHost *:80`
	14.1. Para cada host virtual que se requiera implementar se debe realizar su correspondiente definición
	`<VirtualHost *:80>`
	`DocumentRoot <<directorio asociado>>`
	`ServerName <<nombre asociado>>`
	`CustomLog logs/<< nombre asociado >>-access.log combined`
	`RewriteEngine on`
	`RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)`
	`RewriteRule .* - [F]`
	`RewriteRule ^(.*).asp$ /$.php [L,NC]`
	`</VirtualHost>`
	15. Para cada host virtual modificar los permisos de usuario.
	`#cd /var/www`
	`#chmod 750 html`
	`#chgrp –R apache html`
	15.1. Lo mismo se realizará para cada host virtual
	`#cd /home`
	`#chmod 750 <<directorio_usuario>>`
	`#chgrp –R apache <<directorio_usuario>>`
	`#cd <<directorio_usuario>>`
	`#mkdir html`
	`#chown –R <<directorio_usuario>> html`
	`#chown –R apache html`
	`#chmod 750 html`
	16. Guardar los cambios

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.2 CONFIGURACION DE PHP

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Realizar una configuración específica y especializada en el servidor PHP de la División de Estudios de Posgrado de la Facultad de Economía a fin de minimizar el riesgo de ataques y con ello asegurar la continuidad de la operación.

POLITICAS

1. Modificar la configuración por default para evitar vulnerabilidades conocidas para la última versión del sistema.

2. Ocultar el mayor número posible de información que puede proporcionar el servidor al ocurrir algún error.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.2 CONFIGURACION DE PHP

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD

ADMINISTRADOR DEL SERVIDOR PHP	1. Editar el `php.ini`
	2. Activar el safemode
	`safe_mode = On`
	`safe_mode_grid = Off`
	`safe_mode_include_dir =`
	`safe_mode_exec_dir =`
	3. Deshabilitar se muestre la versión de PHP `expose_php = Off`
	4. Habilitar sólo la notificación de errores graves de php
	`;error_reporting = E_ALL & ~E_NOTICE`
	`Error_reporting =`
	`E_COMPILE_ERROR|E_ERROR|E_CORE_ERROR`
	`;error_reporting = E_ALL`
	4.1. Aunado a esta configuración se debe indicar, explícitamente
	`Display_errors = Off`
	5. Desactivar el register_globals
	`register_globals = Off`
	6. Asegurar que exista la siguiente línea
	`allow_url_fopen = Off`
	7. Validar el squirrelmail
	`#cd /usr/share`
	`#chown –R <<apache>> squirrelmail`
	8. Guardar los cambios

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.3 SEGURIDAD Y ACCESO A LA BASE DE DATOS DE LOS SISTEMAS DE INFORMACION

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener actualizada la información referente a los usuarios de los sistemas de información de la División de Estudios de Posgrado de la Facultad de Economía.

Mantener actualizada la información referente a los privilegios otorgados a los usuarios de los sistemas.

POLITICAS

1. Toda modificación al catálogo de usuarios de los Sistema de Información de la DEP-FE será realizada por el administrador de sistemas a petición expresa del Jefe de la División o del Secretario Académico.

2. Los privilegios de acceso asociados a los usuarios del sistema serán determinados por el Jefe de la División o el Secretario Académico.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.3 SEGURIDAD Y ACCESO A LA BASE DE DATOS DE LOS SISTEMAS DE INFORMACION

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
ADMINISTRADOR DE SISTEMAS DE INFORMACION DE LA DIVISION DE ESTUDIOS DE POSGRADO	1. Obtiene notificación del Jefe de División o Secretario Académico de un nuevo usuario de sistemas. 2. Inserta los datos del nuevo usuario en el catálogo de Usuarios. 3. Realiza pruebas de acceso y niveles de acceso del nuevo usuario en las opciones del sistema. 3.1. En caso de error, revisa los datos ingresados y repite paso 3 a fin de dar el acceso solicitado al nuevo usuario. PARA EL CASO DE MODIFICACION DE PERMISOS, 4. Recibe notificación del Jefe de División o Secretario Académico de modificar los privilegios de acceso a un usuario específico. 5. Realiza la modificación en el catálogo Usuarios. 6. Revisa que el cambio se vea reflejado en todas las opciones para las cuales se modificó el permiso de acceso. 6.1. En caso de error, repite pasos 5 y 6 a fin de obtener un funcionamiento aceptable del sistema.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION
PROCEDIMIENTO 1.4 DESARROLLO DE SISTEMAS

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/3
01	01	2009	

OBJETIVOS

Proporcionar a los responsables de área de la División de Estudios de Posgrado una herramienta que les permita registrar y consultar la información referente a las actividades realizadas por la Planta Docente y los avances de los alumnos inscritos en el Programa de Posgrado en Economía, sede Facultad de Economía.

Proporcionar a los responsables de área apoyo documental confiable para los casos en que realizan conciliación de actividades académicas y administrativas de la DEP-FE.

POLITICAS

1. El desarrollo de sistema será realizado por el Técnico Académico adscrito a la Jefatura de la División de Estudios de Posgrado.

2. Toda adecuación al sistema deberá ser realizada a petición expresa del responsable del área correspondiente realizando a su vez la verificación de su funcionamiento bajo los criterios expresados.

3. Toda modificación al sistema deberá ser documentada a fin de mantener un código legible para su mantenimiento.

4. Toda modificación al sistema deberá ser documentada en el Manual Técnico del mismo a fin de mantener actualizado dicho documento.

5. El código fuente de los sistemas de información desarrollados residirá en la máquina del desarrollador manteniendo una copia en el Centro de Cómputo de la DEP-FE.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION
PROCEDIMIENTO 1.4 DESARROLLO DE SISTEMAS

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/3
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
RESPONABLE DEL DESARROLLO DE SISTEMAS DE INFORMACION DE LA DEP-FE	1. Recibe la política de funcionamiento del sistema por parte del responsable del área. 2. Analiza la problemática en busca de una solución óptima tomando en consideración la normatividad administrativa vigente, el manejo de información dentro de la base de datos y el impacto técnico y práctico de la implementación. 2.1. En caso de no quedar clara la petición, se solicitará al responsable expresar en mayor detalle el funcionamiento que espera por parte del sistema. 3. Determina el código a implementar y realiza la codificación correspondiente; si es el caso, consigna la implementación en el Manual del Sistema correspondiente. 4. Implementa, si es que procede, la misma funcionalidad en opciones asociadas a fin de mantener concordancia dentro del sistema. 5. Realiza las pruebas necesarias a fin de obtener un comportamiento por parte

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.4 DESARROLLO DE SISTEMAS

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	3/3
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
RESPONABLE DEL DESARROLLO DE SISTEMAS DE INFORMACION DE LA DEP-FE	7. Transfiere el código fuente al servidor de operación. 8. Comprueba que el sistema funcione correctamente. 8.1. En caso de error, repite pasos 7 y 8 hasta obtener una versión funcional en la red. FIN DEL PROCEDIMIENTO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.5 MANTENIMIENTO DE CATAOGOS DE LOS SISTEMAS DE INFORMACION DE LA DIVISION DE ESTUDIOS DE POSGRADO

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener actualizados los contenidos de los diversos catálogos utilizados por los sistemas a fin de proporcionar información confiable y oportuna a los responsables de área de la División de Estudios de Posgrado durante la ejecución cotidiana de sus actividades.

POLITICAS

1. La actualización de catálogos la realizará el responsable del desarrollo de Sistemas de Información.

2. La actualización del contenido de los catálogos del sistema se realizará respetando la nomenclatura definida para el registro de información.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.5 MANTENIMIENTO DE CATAOGOS DE LOS SISTEMAS DE INFORMACION DE LA DIVISION DE ESTUDIOS DE POSGRADO

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
RESPONSABLE DEL DESARROLLO DE SISTEMAS DE INFORMACION DE LA DIVISION DE ESTUDIOS DE POSGRADO DE LA FACULTAD DE ECONOMIA	1. Determina la información que será modificada o anexada. 2. Realiza la modificación o incorporación en el catálogo respectivo. 3. Revisa que el cambio sea visualizado en todas las opciones y sistemas que utilicen dicho catálogo. 3.1. En caso de error, repite pasos 2 y 3 a fin de obtener un funcionamiento aceptable de los sistemas. 4. Documenta la modificación realizada. 4.1. En caso de ser necesario, notifica verbalmente al Jefe de División o responsable del área solicitante que la modificación fue realizada. FIN DEL PROCEDIMIENTO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.7 ACTUALIZACION DE ANTIVIRUS DE MANERA REMOTA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener libre de virus, gusanos, troyanos y spyware los equipos de cómputo personales dentro de la División de Estudios de Posgrado de la Facultad de Economía

Contar con una herramienta que permita escanear y desinfectar los equipos de cómputo, memorias y equipos portátiles de la División de Estudios de Posgrado

Mantener actualizado el software antivirus institucional

POLITICAS

1. El software antivirus deberá ser actualizado diariamente

2. Todo equipo de cómputo tendrá un acceso directo a la actualización de la base de datos antivirus

3. La actualización del antivirus es responsabilidad del usuario del equipo

4. Cada uno de los técnicos académicos del Centro de Cómputo deberá contar con un juego de vacunas actualizadas, siendo su responsabilidad la actualización de las mismas

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.7 ACTUALIZACION DE ANTIVIRUS DE MANERA REMOTA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
PERSONAL DE ACTUALIZAR LA VERSION DEL ANTIVIRUS EN EL CENTRO DE COMPUTO	1. Revisa el sitio de Internet a fin de obtener la última versión de la vacuna utilizada por el Centro de Cómputo y personal de la DEP-FE. 2. Transfiere las actualizaciones de vacunas a la carpeta compartida en los equipos de cómputo denominados CubTec1. 3. Anotar en el listado de control de actualización de vacunas la fecha, versión y nombre de la vacuna, así como el nombre de la persona que está realizando la actualización. 4. Crear un juego de discos flexibles o memoria USB con la vacuna correctamente actualizada. 4.1. En caso de aparecer un virus de rápida expansión, se utilizará este juego de discos para proceder a su desinfección. 5. Revisar diariamente el equipo utilizado para verificar los dispositivos utilizados en el salón y laboratorio de cómputo. 5.1. En caso de encontrar archivos en cuarentena, eliminarlos.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.8 PRESTAMO DEL LABORATORIO DE ECONOMETRIA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/4
01	01	2009	

OBJETIVOS

Proporcionar el Laboratorio de Econometría en las mejores condiciones a fin de que los alumnos puedan realizar las prácticas definidas por el profesor o adjunto.

POLITICAS

1. El horario de uso del Laboratorio de Econometría es de Lunes a Viernes de 9:00 a 19:00 horas.

2. El Laboratorio de Econometría sólo podrá ser prestado previa solicitud al Centro de Cómputo.

3. El Laboratorio de Econometría cuenta con 13 (trece) equipos de cómputo útiles.

4. El Laboratorio de Econometría no cuenta con plumones y borrador para pizarrón blanco, por lo que el profesor o adjunto deben traer consigo estos aditamentos para impartir su clase.

5. El préstamo del Laboratorio de Econometría se cancelará en caso de que el profesor utilice plumones indelebles en el pizarrón.

6. Queda estrictamente prohibido introducir alimentos y/o bebidas al Laboratorio de Econometría.

7. Cualquier dispositivo de almacenamiento a utilizar en el laboratorio debe ser previamente verificado y desinfectado por personal del Cetro de Cómputo.

8. Sólo el profesor o adjunto podrán solicitar la apertura del Laboratorio de Econometría.

9. El Laboratorio de Econometría, una vez abierto, no podrá ser abandonado por el profesor o adjunto hasta que personal del Centro de Cómputo esté presente para cerrarlo.

10. Queda estrictamente prohibido navegar por Internet o chatear durante el tiempo

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.8 PRESTAMO DEL LABORATORIO DE ECONOMETRIA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/4
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
PROFESOR O ADJUNTO	1. Solicita en préstamo el Laboratorio de Econometría indicando • Nombre de la materia o curso • Fecha de inicio y término • Horario • Software a utilizar • Uso de mini cañón • Directorio de trabajo durante el curso
ENCARGADO DEL REGISTRO DE SOLICITUDES DEL LABORATORIO DE ECONOMETRIA	2. Recibe la solicitud de préstamo del Laboratorio de Econometría. 3. Revisa que no haya sido previamente asignado el Laboratorio 3.1. En caso de estar asignado a otro curso o evento, notificar el hecho al Profesor o Adjunto. Repetir pasos 1 a 3.
PROFESOR O ADJUNTO	4. Registra solicitud de uso del Laboratorio en el archivo correspondiente. 5. Regresa al Centro de Cómputo el día indicado en la solicitud de préstamo del Laboratorio de Econometría.
PERSONAL DEL CENTRO DE COMPUTO	6. Solicita a personal del Centro de Cómputo la apertura del Laboratorio de Econometría

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.8 PRESTAMO DEL LABORATORIO DE ECONOMETRIA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	3/4
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
PROFESOR O ADJUNTO	9. Notifica al personal del Centro de Cómputo que ya se terminó de utilizar el Laboratorio de Econometría
PERSONAL DEL CENTRO DE COMPUTO	10. Desconecta el minicañon, si es que se ocupó 10.1. En caso de que el minicañón sea entregado por el profesor o ayudante, el personal del Centro de Cómputo revisará que todos los cables (de potencia y de conexión al CPU) estén debidamente almacenados. 11. Revisa los equipos contra virus, troyanos o programas distintos a los específicos para la clase. 11.1. En caso de encontrar este tipo de archivos se notifica al profesor o adjunto a fin de detectar a la persona infractora y aplicar las sanciones que señala el Centro de Cómputo. 12. Revisa los directorios del disco duro de los equipos 12.1. En caso de encontrar directorios extraños se procede a su eliminación

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.8 PRESTAMO DEL LABORATORIO DE ECONOMETRIA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	4/4
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
PERSONAL DEL CENTRO DE COMPUTO	14. Verifica que todos los equipos cuenten con Mouse y con el dispositivo de movilidad 14.1. En caso de que uno de ellos desaparezca, se levanta el reporte correspondiente, se notifica al profesor o adjunto y se ejecuta la sanción correspondiente 15. Verifica que las ventanas estén perfectamente cerradas a fin de evitar filtraciones de agua y polvo 16. Cierra el Laboratorio de Econometría 17. Coloca las llaves del Laboratorio de Econometría en el lugar destinado para ello

FIN DEL PROCEDIMIENTO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION

PROCEDIMIENTO
1.9 ACTUALIZACIÓN DE CONTENIDOS DE LA PÁGINA WEB DE LA PLANTA ACADEMICA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener actualizado el contenido de la página de la Planta Docente de la DEP-FE a fin de proporcionar información confiable y oportuna de las investigaciones y actividades académicas realizadas por los profesores.

POLITICAS

1. Las modificaciones deberán observar las políticas establecidas en cuanto a diseño de páginas web de la División de Estudios de Posgrado de la Facultad de Economía.

2. Las modificaciones a los contenidos serán realizadas mediante petición expresa del académico en cuestión, por el Jefe de la División o por el Secretario Académico de la Facultad de Economía.

3. La actualización de los contenidos los realizará el responsable del desarrollo de sistemas de la DEP-FE.

4. Toda modificación que no sea realizada por el desarrollador de sistemas de información deberá ser autorizada por éste.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA - PREVENCION
PROCEDIMIENTO 1.9 ACTUALIZACIÓN DE CONTENIDOS DE LA PÁGINA WEB DE LA PLANTA ACADEMICA

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
REPONSABLE DEL DESARROLLO DE SISTEMAS DE INFORMACION DE LA DEP - FE	1. Recibe la petición de modificación de contenidos por parte del académico, Jefe de División o Secretario Académico de la Facultad de Economía. 2. Analiza las modificaciones a fin de determinar una solución óptima en cuanto a diseño. 3. Realiza la modificación considerando las políticas de diseño de páginas. 4. Presenta la(s) modificacion(es) al solicitante a fin de obtener su Vo. Bo. 4.1. En caso de nuevas modificaciones repite pasos 2 a 4 hasta obtener la satisfacción del solicitante. 5. Transfiere el archivo fuente al servidor web. 6. Actualiza la(s) liga(s) correspondiente(s) o reemplaza el archivo respectivo. 7. Valida el correcto funcionamiento del sitio de la Planta Académica de la DEP-FE. 7.1. En caso de error, repite pasos 6 y 7 hasta obtener una versión funcional

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA – EJECUCION

PROCEDIMIENTO
2.1 AUSENCIA DE SERVICIOS DE RED

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener en todo momento el servicio de red a fin de realizar las actividades cotidianas de la DEP-FE.

POLITICAS

1. Todos los usuarios de la red deberán respetar los canales de comunicación y vías establecidas para solicitar la restitución del servicio de red.

2. Se deberá respetar los tiempos que técnicamente se requiera para la restitución del servicio, el cual deberá estar listo en un plazo máximo de un día.

3. Deberá existir estrecha comunicación entre los administradores de servidores de servicios y el administrador de la red interna de la Facultad de Economía.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

2. EJECUCION DEL PLAN DE CONTINGENCIA
PROCEDIMIENTO 2.1 AUSENCIA DE SERVICIO DE RED

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
USUARIO	1. Revisa que la conexión a la red se encuentre correctamente conectada. 2. Revisa que en el área exista el servicio. 2.1. En caso de no existir conexión en el equipo solicita un servicio de revisión de equipo. 2.2. En caso de no haber servicio en el área notifica al responsable del Centro de Cómputo de la DEP-FE.
RESPONSABLE DEL CENTRO DE COMPUTO DE LA DEP-FE	3. Revisa que los servidores estén funcionando. 4. Revisa las conexiones físicas de la red. 4.1. En caso de continuar sin servicio notifica al personal del CIFE.
RESPONSABLE DE LA INTERNA DE LA FE	5. Revisa los dispositivos de conexión de la DEP-FE. 6. Soluciona el problema. 7. Reinicia el dispositivo de conexión.
RESPONSABLE DE SERVIDORES DE LA DEP-FE	8. Valida la correcta configuración de los servidores.
RESPONSABLE DEL CENTRO DE	9. Valida la existencia del servicio en todos

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

1. PLAN DE CONTINGENCIA – EJECUCION

PROCEDIMIENTO
2.2 AUSENCIA DE SERVICIOS WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	1/2
01	01	2009	

OBJETIVOS

Mantener en todo momento el servicio web a fin de realizar las actividades cotidianas asociadas a los sistemas de información de la DEP-FE.

POLITICAS

1. Los sistemas de información de la DEP-FE deberán estar siempre disponibles.

2. Los responsables de áreas operativas reportarán al desarrollador de sistemas de información cuando alguno de ellos no se encuentre disponible.

3. Se deberá respetar los tiempos que técnicamente se requiera para la restitución del servicio, el cual deberá estar listo en un plazo máximo de un día.

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO
FACULTAD DE ECONOMIA
DIVISION DE ESTUDIOS DE POSGRADO
MANUAL DE PROCEDIMIENTOS

2. PLAN DE CONTINGENCIA - EJECUCION

PROCEDIMIENTO
2.2 AUSENCIA DE SERVIDOR WEB

REFERENCIA			PAGINA
FECHA DE			
DIA	MES	AÑO	2/2
01	01	2009	

DESCRIPCION

INTERVENCION	ACTIVIDAD
USUARIO	1. Revisa que el servicio de red funcione correctamente. 1.1. En caso de tener servicio de red pero no el del servidor web, notificar al administrador de servidores de la DEP-FE.
ADMINISTRADOR DE SERVIDORES DE LA DEP-FE	2. Revisa que los servidores estén funcionando de manera correcta. 3. Ejecuta los procesos de reinicio del servidor. 4. Revisa que los servicios estén nuevamente activos. 5. Notifica la existencia del servicio.

FIN DEL PROCEDIMIENTO