UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

BUENAS PRÁCTICAS PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN UN CENTRO DE CÓMPUTO

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

PRESENTA:

LETICIA HERNÁNDEZ SÁNCHEZ

DIRECTORA DE TESIS:

M.C. CINTIA QUEZADA REYES

MÉXICO, D.F. 2014

AGRADECIMIENTOS

A mis padres que siempre me han apoyado y orientado, gracias por los esfuerzos y sacrificios para darme la mejor herencia, mi educación en la mejor universidad.

A mis hermanos que siempre me han brindado su amistad y comprensión.

A la Facultad de Ingeniería de la Universidad Nacional Autónoma de México por haberme brindado una formación académica, profesional y humana. Es un gran orgullo y honor ser parte de la máxima casa de estudios.

A cada uno de mis profesores, gracias por sus enseñanzas para mi formación profesional.

A la M.C. Cintia Quezada Reyes, por su apoyo en la elaboración de esta tesis.

A mis amigos y compañeros de trabajo.

ÍNDICE

INTRODUCCIÓN

Actualmente hay diferentes tipos de tecnologías las cuales van en aumento, dejando atrás la parte de seguridad en la información y en los distintos dispositivos con los que se cuenta. Por ejemplo, el caso de computadoras, celulares, tabletas, impresoras, etcétera.

En este tipo de dispositivos continúan surgiendo problemas de seguridad, debido a la falta de interés por parte de los usuarios, por no identificar la importancia de resguardar su información o datos personales, o simplemente al no elaborar una buena contraseña para sus correos electrónicos, cuentas bancarias, etcétera. En algunos casos hay filtros de información confidencial y personal, como colocar datos personales en encuestas, en páginas de redes sociales, fotografías, ubicación, posesión de bienes materiales, entre otros datos.

Dando como resultado un gran número de huecos en seguridad, los cuales se pueden corregir con atenciones y cuidados, por ejemplo en un centro de cómputo, con un listado de buenas prácticas y políticas de seguridad. Esos huecos de seguridad, también se deben a la falta de comunicación y de capacitación de los interesados los cuales se convierten en el eslabón más débil en la cadena de seguridad.

Por lo cual, en el siguiente trabajo se describen las responsabilidades de cada integrante del centro de cómputo y las recomendaciones que deben seguir los interesados.

Este trabajo escrito, es un conjunto de recomendaciones basadas en la experiencia, en algunas políticas de seguridad y en un estándar para el control de la tecnología de la información, como lo es COBIT. Con el fin de proporcionarles a los usuarios, encargados y administradores, temas actuales de seguridad en la información y en el centro de cómputo, dando como resultado la certeza de que se está asegurando lo mejor posible.

En este trabajo, se tienen como objetivos:

- Diseñar buenas prácticas para la seguridad del centro de cómputo.
- Proporcionar buenas prácticas de seguridad física y perimetral a los integrantes en el centro de cómputo.
- Promover el concepto de seguridad.
- Promover la importancia de las buenas prácticas entre los administradores y usuarios.
- Difundir las buenas prácticas en el centro de cómputo.

Se pretende evaluar el conocimiento en un centro de cómputo, desde la organización, servicios de seguridad y las tareas de los principales autores en el centro de cómputo, mecanismos de seguridad, entre otras actividades, esto para brindar una mejor seguridad interna y externa en el centro de cómputo.

Al identificar y analizar los servicios en el centro de cómputo, se van elaborando medidas preventivas, como realizar un análisis para detectar los posibles riesgos, implementando cierto grado de seguridad en los servicios del centro de cómputo, así como controles que ayudan a proporcionar un mejor entorno en la seguridad del centro de cómputo.

Se brinda la importancia de identificar y comprender las políticas de seguridad y las buenas prácticas, saber que para cada recurso hay lineamientos a seguir. Y la importancia de la información para tomar las medidas necesarias e impedir su pérdida.

Se encuentra también una metodología propuesta, que contiene conceptos como: seguridad, vulnerabilidades y amenazas de igual manera la forma de la estructura de la organización y los diferentes dispositivos en el centro de cómputo por medio de una encuesta para identificar el estado inicial o actual del centro de cómputo con sus respectivos requerimientos.

Con la información recopilada en este trabajo se pretende proporcionar una guía para la implementación de la seguridad en los centros de cómputo, así como también promover el concepto de seguridad, difundiendo las buenas prácticas con diferentes métodos, para que los integrantes del centro las conozcan y las lleven a cabo.

El principal objetivo de este trabajo es proporcionarle al lector ideas, métodos y estrategias para el diseño, elaboración, implementación, retroalimentación y difusión de las buenas prácticas de seguridad para optimizar la manera en que se resguarda la información y el lugar de trabajo.

CAPÍTULO 1

CONCEPTOS BÁSICOS

1.1 DEFINICIONES

1.1.1 ADMINISTRACIÓN

Las organizaciones en su dimensión como entes sociales tienen como prioridad el uso racional de sus recursos, es decir, el uso de cada uno de sus insumos (financieros, económicos, técnicos, humanos, etcétera) de forma óptima y útil. El responsable suele ser un administrador al cual se le exige disponibilidad absoluta, integridad moral, estudios especializados y actualizados, conocimiento de la naturaleza humana, finalidad y asertividad en la toma de decisiones, tacto y calidez en las relaciones interpersonales.

Según F. Tannenbaum, se define a la administración como: "El empleo de la autoridad para organizar, dirigir y controlar subordinados responsables, con el fin de que todos los servicios que se presentan sean debidamente coordinados en el logro del fin de la empresa", es decir, es el proceso que pretende diseñar los objetivos que deben lograr un grupo de personas, controlando los medios que utilizan. [1]

La administración se contempla como una disciplina orientada al cumplimiento de objetivos organizacionales mediante la coordinación del esfuerzo humano y de recursos materiales, financieros y tecnológicos.

La administración es la actividad humana que tiene como objetivo coordinar los recursos con los que cuenta una organización, lograr en forma eficiente y satisfactoria los objetivos individuales e institucionales.[2]

Al administrar un centro de cómputo se requiere un modelo de proceso administrativo. Actualmente la división más aceptada y la más utilizada de este modelo es: planeación, organización, dirección y control. (Figura 1.1)

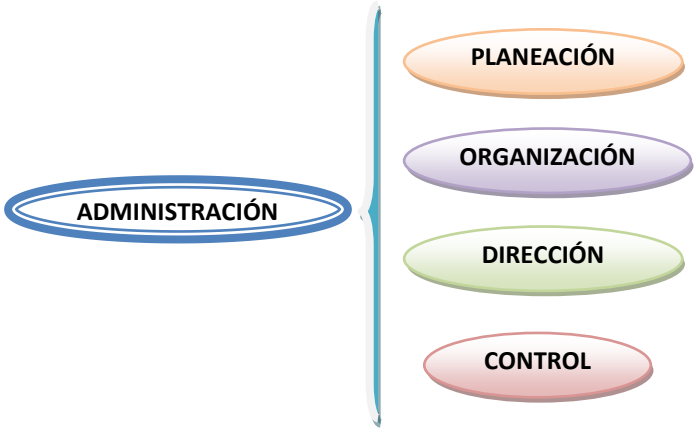

Figura 1.1 Principales funciones de la administración

[1]Francisco Hernández Mendoza. Administración Básica I. UNAM, FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN. Fondo Editorial, 2003. Página 22

[2] *Íbid*. Página 28

A continuación se detallarán las principales funciones de la administración.

1) PLANIFICACIÓN

Según Heriberto Olguín en su libro Organización y Administración de Centros de Cómputo. "La planificación es un proceso mediante el cual determinamos de dónde venimos, en qué situación estamos, a dónde queremos ir y cómo y cuándo llegaremos allí". [3]

Esta etapa es el proceso de toma de decisiones, se entiende como puente entre el presente y un futuro deseado. Se definen también los objetivos y la forma de pasar del sistema presente al futuro, así como los medios utilizados.

La planificación no se ocupa de las decisiones futuras, sino del impacto futuro de las decisiones actuales. Al planificar, se trabaja hacia atrás desde los objetivos para decidir qué se debe hacer ahora cuando se acerque una fecha futura.

La planificación no está encaminada a eliminar el riesgo -asumir riesgos es esencial para el progreso- sino a asegurar que se aceptan los riesgos oportunos en el momento oportuno.

La planificación está orientada a garantizar el uso eficaz de los recursos disponibles para el logro de los objetivos más importantes. Tiende a prevenir la crisis antes de que aparezca.

En este proceso de planificación se fijan los objetivos específicos y medibles al igual que las estrategias y políticas, estableciendo así, la base para el control. Esto usando como herramienta el mapa estratégico, que provee un lenguaje para describir la estrategia, antes de elegir las métricas para evaluar su desempeño. Todo esto teniendo en cuenta las fortalezas / debilidades de la organización y las oportunidades / amenazas del contexto, es decir, el análisis DAFO.

El análisis DAFO, también conocido como FODA, es una metodología de estudio de la situación de una empresa o un proyecto, analizando sus características internas (Debilidades y Fortalezas) y su situación externa (Amenazas y Oportunidades).

El método del análisis FODA es apropiado para ordenar el pensamiento e información, facilitando la comprensión y la evaluación de la situación inicial y su posible evolución.

Al realizar este análisis se identifican los aspectos positivos y negativos de la situación interna y externa de la organización. (Figura 1.2)

[3] Heriberto Olguín. Organización y Administración de Centros de Cómputo. Versión digital. Página 23.

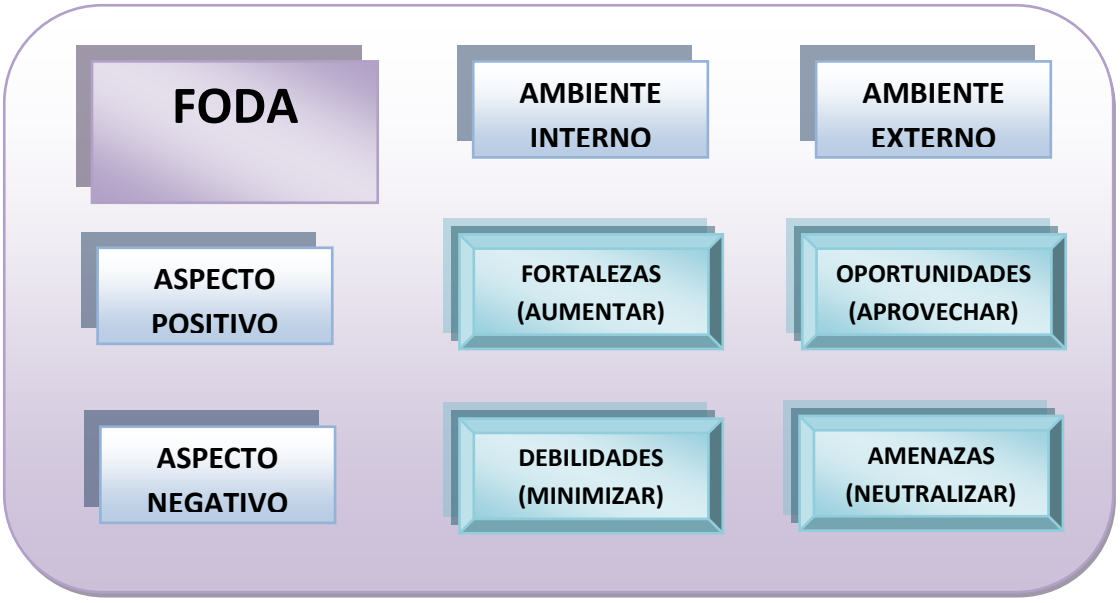

Figura 1.2 Aspectos del ambiente interno y externo del análisis FODA

El análisis FODA sirve como guía, ya que muestra el punto de inicio y ayuda a potenciar las fortalezas de grupo y planificar cómo aprovechar las oportunidades.

De igual manera, se puede realizar el análisis FODA personal de cada integrante con el propósito de contribuir a un excelente desempeño como equipo de trabajo.

A continuación se presenta un ejemplo de análisis FODA personal. (Figura 1.3)

Figura 1.3 Análisis FODA personal

La utilidad del análisis FODA es desarrollar un plan que tome en consideración muchos y diferentes factores internos y externos para así maximizar el potencial de las fuerzas y oportunidades minimizando así el impacto de las debilidades y amenazas. Se debe de utilizar al desarrollar un plan estratégico o al planear una solución específica a un problema.

Este análisis es una herramienta para conocer la situación real en que se encuentra una organización, empresa o proyecto y planificar una estrategia de futuro. Durante la etapa de planificación estratégica y a partir del análisis FODA se deben contestar las siguientes preguntas:

- ¿Cómo se puede explotar cada fortaleza?
- ¿Cómo se puede aprovechar cada oportunidad?
- ¿Cómo se puede detener cada debilidad?
- ¿Cómo se puede defender de cada amenaza?

Para efectuar un adecuado estudio con el uso del análisis FODA, se debe considerar el impacto potencial de un factor problemático, ya sea interno o externo, sobre la empresa o su estrategia.

2) DIRECCIÓN

En la dirección se considera la planificación y la organización para mejorar la forma de obtener los objetivos. Dirigir es la capacidad de decidir, tener el liderazgo sobre los individuos para la obtención de los objetivos fijados. Tomar decisiones usando modelos lógicos e intuitivos. En esta etapa se deberán conocer completamente los planes, metas y objetivos organizacionales. No sólo basta con conseguir los objetivos, sino que hay que conseguirlos con el menor número de recursos.

El objetivo de la dirección es alcanzar el máximo rendimiento de todos los empleados en el interés de los aspectos globales. Encauza todos los esfuerzos de los subordinados hacia el objetivo en común. Subordina los intereses del grupo de trabajadores a los intereses de la empresa.

Una de sus principales tareas de esta fase es supervisar que se esté realizando conforme a lo planeado. Incluye la motivación a los subordinados, la conducción de otros, la selección de los canales de comunicación más efectivos y la resolución de conflictos.

Por mencionar algunas de las tareas del jefe encargado de una dirección se tiene:

- Conocer a fondo su personal
- Estar bien informado en cuanto a los acuerdos que obligan al negocio y a sus empleados
- Conducir inspecciones periódicas del cuerpo social ayudándose con cuadros sinópticos (cartas organizacionales).
- Promover en el personal la iniciativa y el empeño.

3) CONTROL

La dirección puede no concluir sino continuar. Después de comprobar el estado de los objetivos se continúa con la etapa de control. Esta etapa también es conocida como evaluación ya que se mide

el desempeño de lo ejecutado, comparándolo con los objetivos y metas fijadas; se detectan los desvíos y se toman las medidas necesarias para corregirlos.

El control permite determinar si se lograron los objetivos o resultados esperados por el departamento, dando inicio a nuevas metas, objetivos y estrategias que vayan de la mano con los objetivos organizacionales.

El control consiste en una verificación para comprobar si todas las cosas ocurren de conformidad con el plan adoptado, las instrucciones transmitidas y los principios establecidos. Su objetivo es localizar los puntos débiles y los errores para rectificarlos y evitar su repetición. Se aplica a todo: a las cosas, a las personas, a los actos.

Las personas que llevan a cabo esta tarea se les llaman verificadores o inspectores. El buen verificador debe ser competente e imparcial. El ser competente no necesita demostración ya que tiene un don para juzgar acerca de la calidad de un objeto, de la calidad de los escritos, etcétera. Para ser imparcial se debe tener una conciencia recta, además debe existir una completa independencia del interventor respecto al intervenido.

El control se realiza a nivel estratégico, nivel táctico y a nivel operativo; la organización entera es evaluada mediante un sistema de control de gestión; por otro lado, también es recomendable contratar auditorías externas, donde se analizan y evalúan las diferentes áreas funcionales de la organización.

A continuación, se resumirán las principales funciones de la administración. (Figura 1.4)

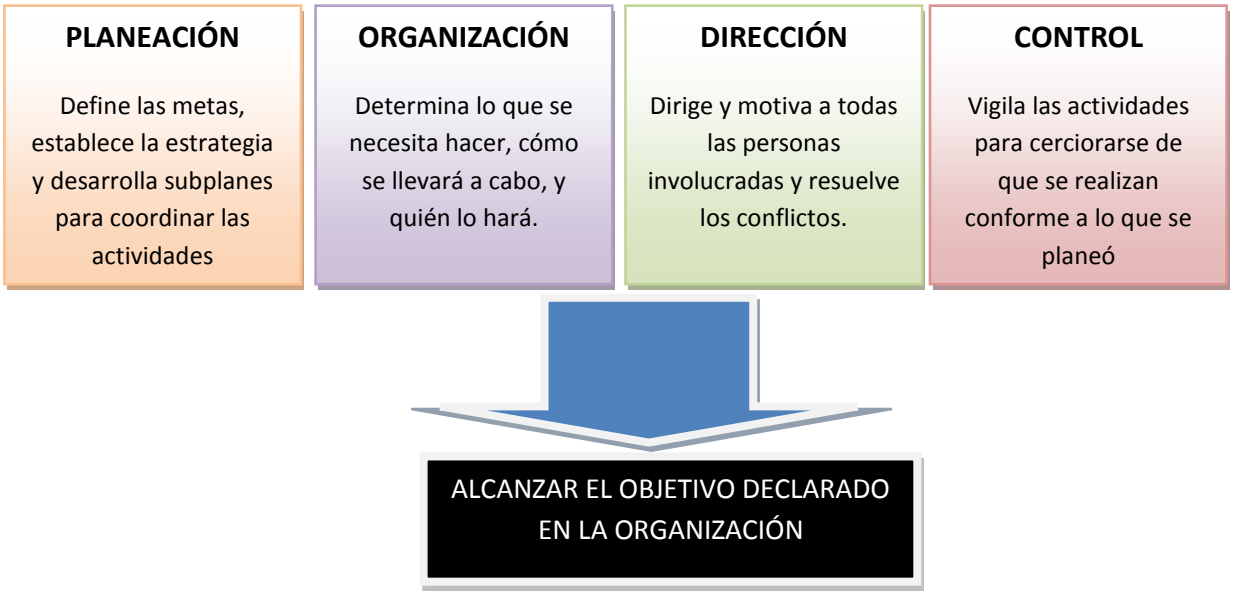

Figura 1.4 Funciones de la Administración

El control de gestión es un proceso que sirve para guiar la gestión empresarial hacia los objetivos de la organización y un instrumento para evaluarla.

Para evaluarla se requiere un buen sistema de gestión de calidad, el cual contiene la planificación de gestión de la calidad, el control de la gestión de la calidad y la mejora continua de gestión de la calidad. (Figura 1.5)

Figura 1.5 Sistema de gestión de calidad

1.1.2 ORGANIZACIÓN

En la administración de un centro de cómputo, es importante definir los objetivos de su diseño en metas presentes y futuras, así como también se debe conocer la finalidad de su creación y a quiénes va dirigido. Ya que se cuenta con la etapa de planificación, el siguiente paso será la organización.

Según Heriberto Olguín en su libro Organización y Administración de Centros de Cómputo, desde el punto de vista empresarial puede definirse a la organización como la aplicación de un conjunto de técnicas conducentes para obtener una empresa estructurada en forma tal, que con la correspondiente división de actividades y la debida coordinación de éstas, se obtenga la máxima rentabilidad. La organización es la fase de la labor del administrador que tiende a adecuar los recursos previstos en la planificación para conseguir los objetivos.[4]

[4] *Íbid.* Página 35.

La organización tiende a estructurar la empresa creando órganos con funciones distintas, pero coordinados todos ellos entre sí para obtener el último fin de la empresa, que es el beneficio y el progreso. Establece la estructura de la empresa, determina relaciones, describe puestos de trabajo, califica estos puestos, etcétera.

La organización, determina cuáles son las actividades a realizar, quiénes las llevarán a cabo, cómo deben agruparse éstas, quién informa a quién y dónde se tomarán las decisiones.

Las finalidades que tiene la organización es el cumplimiento de los objetivos, obtener el máximo aprovechamiento posible de los recursos y simplificar las funciones del grupo social.

En la organización se asignan las tareas y se coordina el trabajo de los empleados, cuyo resultado es la estructura formal de la empresa. En esta etapa se produce la división del trabajo que conlleva la coordinación de esfuerzos, se definen las relaciones entre personas y unidades entre la organización y el exterior.

La importancia que tiene la organización en el centro de cómputo es la siguiente:

- Establecer la mejor manera de alcanzar los objetivos.
- Suministrar los métodos para que se puedan desempeñar las actividades eficientemente con el mínimo de esfuerzo.
- Reducir o eliminar la duplicidad de esfuerzos al delimitar funciones y responsabilidades.

Al organizar el centro de cómputo se considerarán las siguientes etapas para obtener el máximo aprovechamiento posible de los recursos y simplificar las funciones del grupo social.

a) División del trabajo.
   Es la separación y delimitación de las actividades con el fin de realizar una función con la mayor precisión, eficiencia y mínimo de esfuerzo, dando lugar a la especialización y perfeccionamiento del trabajo.

b) Sistematización.
   Esto se refiere a que todas las actividades y recursos de la empresa deben de coordinarse racionalmente a fin de facilitar el trabajo y la eficiencia.

c) Jerarquización.
   Se refiere a la disposición de funciones por orden de rango, grado o importancia.

d) Departamentalización.
   Es la división o agrupamiento de las funciones y actividades en unidades específicas con base en su similitud.

e) Descripción de funciones, actividades y responsabilidades.
   Es la recopilación ordenada y clasificada de todos los factores y actividades necesarias para llevar a cabo el trabajo de la mejor manera.

f) Coordinación.
   Se refiere a sincronizar y armonizar los esfuerzos, las líneas de comunicación y autoridad deben ser fluidas y se debe lograr la combinación y la unidad de esfuerzos bien integrados y balanceados en el grupo social.

g) Simplificación de funciones.
   Uno de los objetivos básicos de la organización es establecer los métodos más sencillos para realizar el trabajo de la mejor manera posible.

Esta etapa responde a las preguntas ¿Quién va a realizar la tarea?, implica diseñar el organigrama de la organización definiendo responsabilidades y obligaciones; ¿cómo se va a realizar la tarea?; ¿cuándo se va a realizar?; en definitiva organizar es coordinar y sincronizar.

1.1.3 INFORMACIÓN

Se debe conocer explícitamente el entorno del centro de cómputo, asimismo la información que se va a administrar para brindarle seguridad. A continuación se definirá información, para comprender y realizar una buena administración.

En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Los datos una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo de conocimiento tomar decisiones pertinentes acordes con él.

Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

Aunado a esto se debe tener conocimiento de las fuentes de información. Generalmente se tiene un conocimiento limitado sobre la variedad de fuentes de información que se tienen a disposición para resolver los problemas que con frecuencia se enfrentan y, más aún, sobre las diferentes estrategias que pueden utilizar para acceder a ellas. Del mismo modo, suelen tener dificultades para reconocer si la información que encuentran es útil para atender su necesidad de información y además, si ésta es confiable y de buena calidad.

El objetivo principal es que se desarrollen habilidades de búsqueda y evaluación de fuentes de información, especialmente cuando se utiliza el Internet como medio para acceder a ellas. Para lograr este objetivo, es necesario que:

a) Se conozca gran cantidad de las fuentes a la que pueden acceder, sus tipos y las características de la información que ofrecen.

b) Que se esté en capacidad de seleccionar las fuentes que pueden responder mejor a las necesidades de la información.

c) Que se identifiquen los diferentes tipos de motores de búsqueda, se utilicen adecuadamente y se apliquen estrategias de búsqueda lógica que se ajusten a los parámetros del problema de información.

d) Que se reconozca la importancia de evaluar las fuentes que se encuentren. Y que se adquieran criterios sólidos para juzgar su oportunidad, calidad y confiabilidad.

Al término se debe evaluar el desempeño de cada paso y retroalimentarlos continuamente. (Figura 1.6)

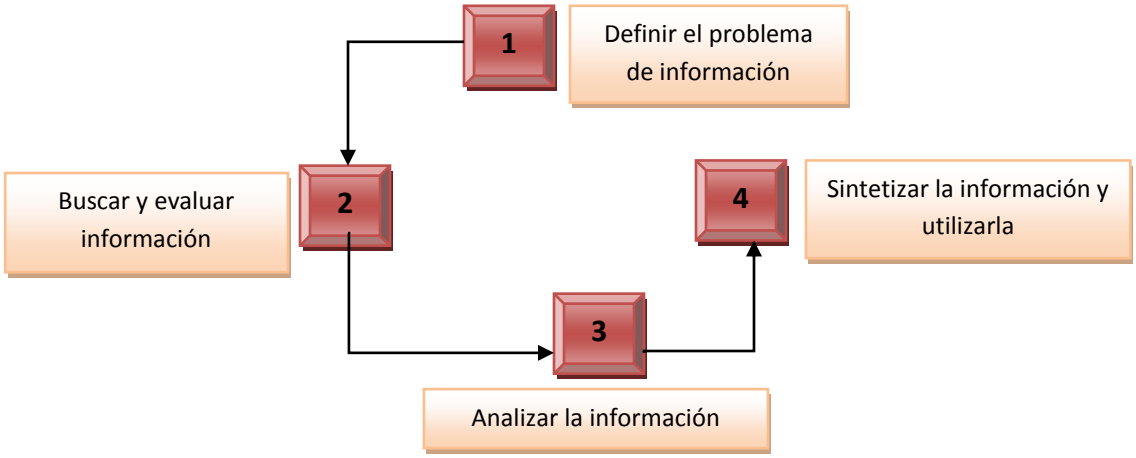

Figura 1.6 Retroalimentación de la información

Para llevar a cabo la retroalimentación se debe:

- Buscar y evaluar la información.
- Identificar y seleccionar las fuentes de información.

En resumen, la información constituye un mensaje sobre un cierto fenómeno o ente, que tiene un significado para alguien o algo.

Se considera que la generación y/o obtención de información persigue estos objetivos:

a) Aumentar/mejorar el conocimiento del usuario, o dicho de otra manera, reducir la incertidumbre existente sobre un conjunto de alternativas lógicamente posibles.
b) Proporcionar a quien toma decisiones la materia prima fundamental para el desarrollo de soluciones y la elección.
c) Proporcionar una serie de reglas de evaluación y reglas de decisión para fines de control.

En relación con el tercer punto, la información como vía para llegar al conocimiento, debe ser elaborada para hacerla utilizable o disponible (este proceso empírico se llama documentación y tiene métodos y herramientas propios), pero también es imposible que la información por sí sola dote al individuo de más conocimiento, es él quien valora lo significativo de la información, la organiza y la convierte en conocimiento.

La información es un activo que tiene valor en la organización y por consiguiente debe ser debidamente protegida. Ya que es importante la información para la organización, se necesita llevar a cabo un procedimiento para resguardarla, es decir, una seguridad.

1.2 SEGURIDAD

1.2.1 SEGURIDAD DE LA INFORMACIÓN

Según María Jaquelina López y Cintia Quezada en su libro Fundamentos de Seguridad Informática: "El término seguridad de la información se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional la transferencia, modificación, fusión o destrucción no autorizada de la información".[5]

La seguridad de la información engloba todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad (conocida como la tríada CIA, del inglés: "Confidentiality, Integrity, Availability") de la misma. (Figura 1.7)

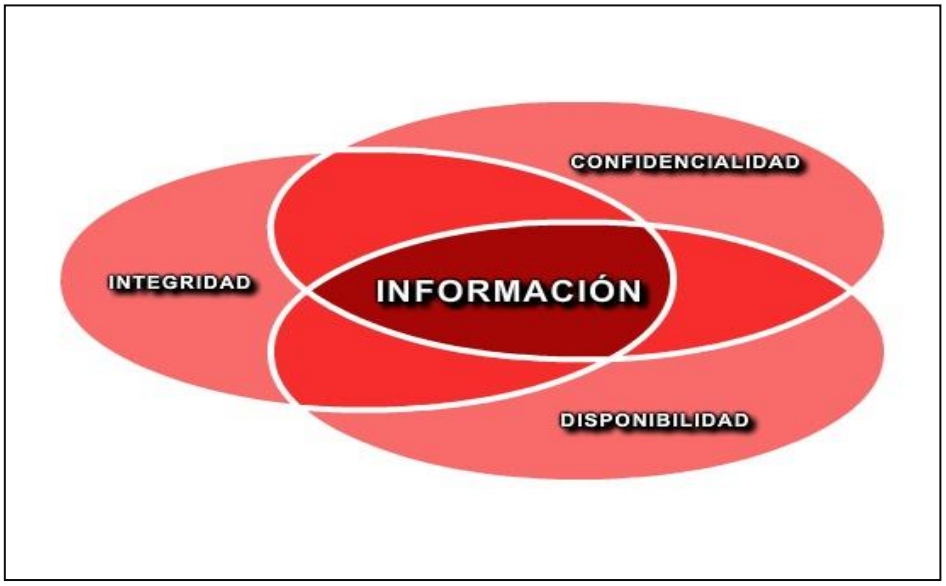

Figura 1.7 Tríada (Confidencialidad-Integridad-Disponibilidad)

[5] María Jaquelina López y Cintia Quezada. Fundamentos de seguridad informática. UNAM. Facultad de Ingeniería, 2006. Página 23

A continuación se explican brevemente los principios básicos de la seguridad de la información.

1. Confidencialidad.- Condición que garantiza que la información es accedida solo por las personas autorizadas según la naturaleza de su cargo o función dentro de la organización. La confidencialidad está relacionada con la *Privacidad de la Información*.

2. Integridad.- Condición que garantiza que la información es consistente o coherente. Está relacionada con la *Veracidad de la Información*.

3. Disponibilidad.- Condición que garantiza que la información puede ser accedida en el momento en que es requerida.

La seguridad de la información debe proteger cada una de estas dimensiones de la información, según su grado de criticidad.

Además, involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto principal el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

En este sentido, es importante conocer no sólo el valor de la información sino el flujo de la información en su transmisión y manejo.

Se considera flujo normal de un emisor a un receptor cuando se envía información desde el emisor y ésta llega a su destino en tiempo, forma y sin alteración. (Figura 1.8)

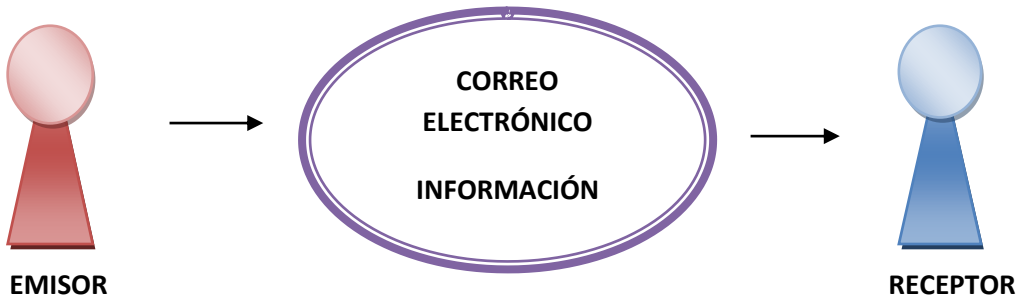

Figura 1.8 Flujo de la información

El flujo de información es importante para determinar los procedimientos y los parámetros de las actividades que se emplean en un proceso.

1.3 AMENAZAS Y VULNERABILIDADES

1.3.1 TIPOS DE AMENAZAS

Según Enrique Daltabuit Godás. "Una amenaza será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema". [6]

Las amenazas son eventos que pueden causar alteraciones a la información, ocasionándole pérdidas materiales, económicas, de información y de prestigio.

Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, pueden provenir de diferentes orígenes: desastres naturales, errores de hardware, de software, de red y amenazas humanas.

a) Desastres naturales

Son eventos que tienen su origen en los fenómenos naturales, el hombre no puede controlar su ocurrencia ni predecirlas. Estos desastres no sólo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etcétera) pudiendo dejarlo en un estado de inoperabilidad permanente. Ejemplos: Inundaciones, terremotos, incendios, huracanes, tormentas eléctricas.

b) Errores de Hardware

Se refiere a las posibles fallas físicas totales o parciales de un dispositivo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, aunque también pueden ser el resultado de un mal uso, descuido en el mantenimiento o término de vida útil. Ejemplos: Errores de fabricación, desgaste de componentes.

c) Software

Existe software de uso malicioso que representa una amenaza directa contra un sistema. Ejemplos: Código malicioso, virus, caballos de Troya, gusanos, errores de programación y diseño.

d) Errores de red

Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red y la extracción lógica de información a través de ésta. Ejemplos: Denegación de servicios, robo de información, intrusos en la red.

[6]Enrique Daltabuit Godás/Leobardo Hernández Audelo. La seguridad de la información. Editorial Limusa, 2007. Página 93

e) Humana

Esta amenaza de tipo humano es ocasionada por ignorancia, diversión, descuido y/o extorsión. Es el tipo de amenaza más común, se conoce que el humano es el eslabón más débil de la seguridad. "Los usuarios son el elemento más difícil de controlar en un sistema informático"

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos. Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados. Ejemplos: Los actos humanos que pueden afectar la seguridad de un sistema. Terroristas, robo, sabotaje, fraude, ingeniería social, ingeniería inversa.

Las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad. Existen amenazas relacionadas con fallas humanas, con ataques malintencionados o con catástrofes naturales. Mediante la materialización de una amenaza podría ocurrir el acceso modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información.

1.3.2 TIPOS DE VULNERABILIDADES

Una vulnerabilidad consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.[7]

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, asimismo, puede causar daños por sí mismo sin tratarse de un ataque intencionado.

Se les consideran elementos internos del sistema, por lo que es tarea de los administradores y usuarios el detectarlas, valorarlas y reducirlas ya que representa las debilidades o aspectos atacables de un sistema informático y pueden ser explotadas por una o varias amenazas.

Las vulnerabilidades pueden clasificarse en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

a) Física (entorno e instalaciones)

Este tipo de vulnerabilidad está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema. Por

[7] *Íbid.* Página 93

ejemplo: instalaciones inadecuadas, ausencia de equipos de seguridad, cableados desordenados y expuestos, falla de identificación de personas, equipos y áreas. Las vulnerabilidades físicas ponen en riesgo a la disponibilidad.

b) Natural

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que causan daño a un sistema. Las vulnerabilidades de tipo natural se presentan, principalmente, en deficiencias de las medidas tomadas para afrontar los desastres. Por ejemplo: mal sistema de ventilación o calefacción.

c) Hardware

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño, etcétera.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo: el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en ese sistema.

Otros ejemplos evidentes son: no verificar las características técnicas de los dispositivos junto con sus especificaciones, la falta de mantenimiento del equipo, adquirir un equipo de mala calidad o hacer un mal uso del mismo, tener el equipo de cómputo expuesto a cargas estáticas.

d) Software

Fallas o debilidades de los programas del sistema hacen más fácil acceder a él. Errores de programación en el sistema operativo o aplicaciones que permiten atacarlo desde la red, explotando la vulnerabilidad en el sistema.

e) Red

Las redes pueden llegar a ser sistemas muy vulnerables. Al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red, la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio. Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

f) Humana

Los elementos humanos de un sistema son los más difíciles de controlar, lo que los convierte en constantes amenazas y, al mismo tiempo, una de las partes más vulnerables del sistema.

Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concientización, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad y mal uso del equipo de cómputo.

Los actos contra la seguridad realizados a conciencia por un elemento humano (como el robo de información o la destrucción de los sistemas) pueden ser el resultado de una vulnerabilidad humana, ya sea por un usuario que accidentalmente revela las contraseñas de acceso o no revisa periódicamente las bitácoras de actividades de los equipos de cómputo a fin de buscar actividades sospechosas por citar algunos ejemplos.

1.4 ATAQUES

Los ataques cibernéticos se están incrementando con mayor frecuencia y cada vez con mayor sofisticación. Las razones principales para atacar una red son:

- Ventajas económicas, corporativas, sabotaje.
- Empleados descontentos, fraudes, extorsiones.
- Espacio de almacenamiento, ancho de banda, servidores de correo (SPAM).

Un ataque se define como cualquier acción que explota una vulnerabilidad. En una comunicación se está expuesto a cuatro categorías de ataque: interrupción, intercepción, suplantación y modificación. [8]

A continuación se muestra el flujo de información correcto (Figura 1.9), así como las diferentes categorías de ataque.

Figura 1.9 Flujo de la información correcto.

[8] *Íbid.* Página 96

a) Interrupción

El principal daño de este ataque es que pierde o deja de funcionar un punto del sistema, su detección es inmediata. Este ataque atenta contra la disponibilidad (Figura 1.10). Algunos ejemplos son: Destrucción del disco duro, borrado de programas o datos, corte de una línea de comunicación.

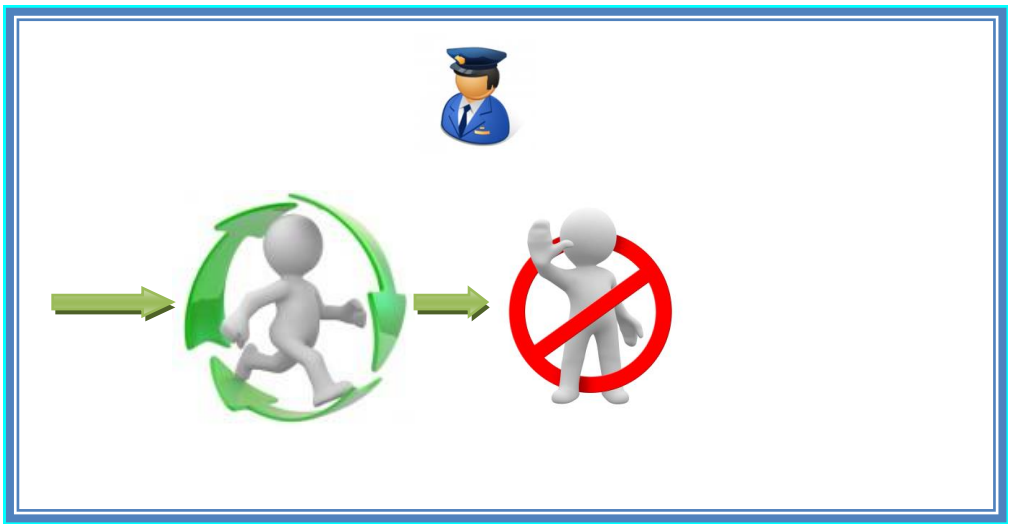

Figura 1.10 Interrupción

b) Intercepción

El principal daño es que se accede a la información por parte de personas no autorizadas, utilizan privilegios no adquiridos. Su detección es difícil y a veces no deja huellas. Este ataque atenta contra la confidencialidad (Figura 1.11). Algunos ejemplos son: Copias ilícitas de programas, escucha en línea de datos.

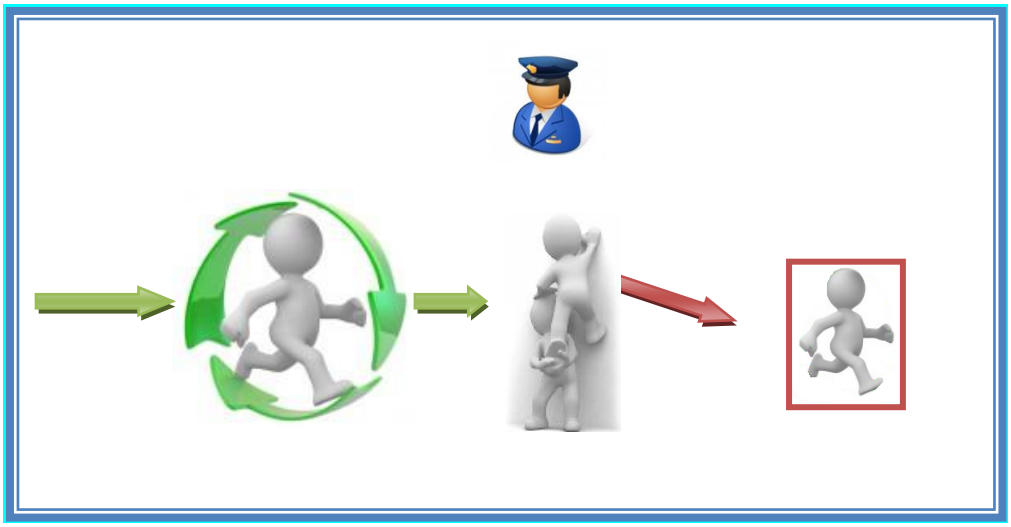

Figura 1.11 Intercepción

c) Suplantación

El principal daño es la sustitución de algo, se hace pasar por alguien. Se crean nuevos objetos dentro de un sistema. Su detección es difícil, la mayoría son delitos de falsificación. Este ataque atenta contra la autenticación (Figura 1.12). Algunos ejemplos son: Introducción de mensajes en una red, añadir registros en una base de datos, creación de páginas web para conseguir los datos de quienes ingresan o acceden al sitio web.

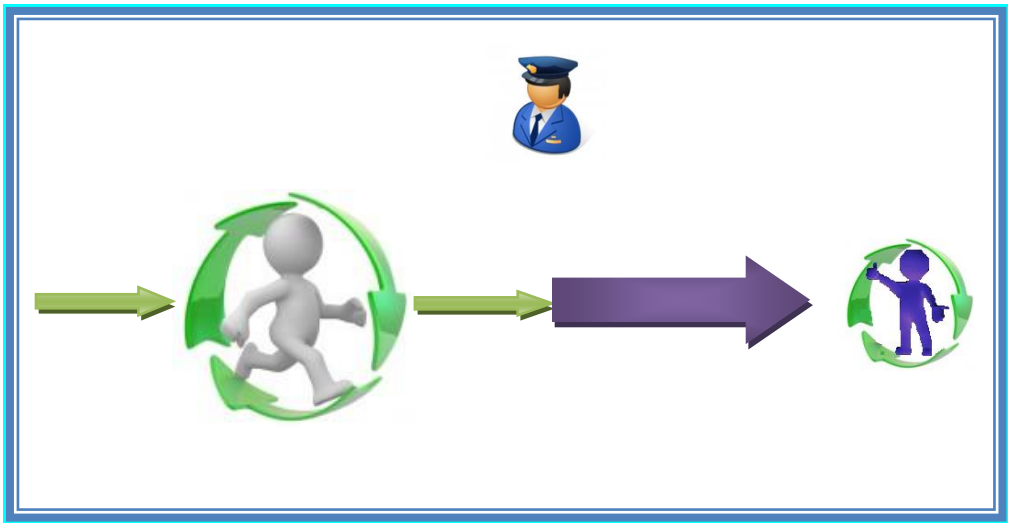

Figura 1.12 Suplantación

d) Modificación

La información ha sido alterada sin permiso. El principal daño es el acceso no autorizado que cambia la información para su beneficio. Su detección es difícil según las circunstancias. Este ataque atenta contra la integridad (Figura 1.13). Algunos ejemplos son: Modificación de bases de datos, modificación de mensajes transmitidos en una red.

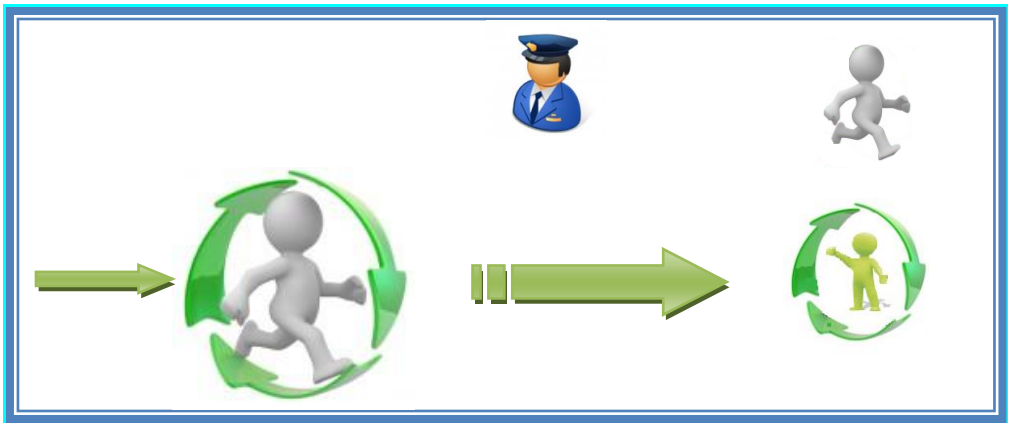

Figura 1.13 Modificación

Pese a todas las medidas de seguridad puede ocurrir un desastre, una amenaza, un incidente o algún tipo de ataque. Los tipos de ataque pueden ser pasivos o activos.

Los ataques activos son acciones iniciadas por una persona que amenaza con interferir el funcionamiento adecuado de una computadora o hace que se difunda de un modo no autorizado. Por ejemplo, el borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

En el ataque pasivo se intenta obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Esto puede dar información importante sobre el sistema.

1.5 SERVICIOS DE SEGURIDAD

Los servicios de seguridad son aquellos que mejoran la seguridad en un sistema de información y el flujo de información de una organización. Están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Son los encargados de que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Además de que nadie pueda interceptar las comunicaciones o los mensajes entre entidades. Son conocidos como los pilares de la seguridad y son:

1) CONTROL DE ACCESO

El control de acceso es la habilidad para limitar y controlar el acceso a los sistemas y aplicaciones mediante los puentes de comunicación. Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que le sea permitido el acceso.

El control de acceso puede ejecutarse de acuerdo con los niveles de seguridad y mediante la administración de la red o por una entidad individual de acuerdo con las políticas de control de acceso. Para llevar a cabo la implementación de esto se utilizan las listas de control de acceso.

Una lista de control de acceso es un conjunto de permisos que determinan quién puede tener acceso a los recursos individuales de la red y qué puede hacerse con los recursos, esta lista deja que el propietario de un recurso permita o deniegue el acceso a los recursos a una entidad o a un grupo de entidades.

2) INTEGRIDAD

La integridad de datos provee controles que aseguran que el contenido de los datos no haya sido modificado y que la secuencia de los datos se mantenga durante la transmisión sin alteración.

3) NO REPUDIO

El no repudio previene a los emisores o receptores de negar un mensaje transmitido. El no repudio se aplica al problema de la denegación falsa de la información que se recibe de otros o de la que uno ha enviado a otros.

4) CONFIDENCIALIDAD

Es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo. Significa mantener la información secreta para proteger los recursos y la información contra el descubrimiento intencional o accidental por personal no autorizado.

5) AUTENTICACIÓN

Verifica la identidad. Este servicio trata de asegurar que una comunicación sea auténtica. Su función es asegurar al receptor que el mensaje provenga de la fuente que espera.

Cuando hay una interacción de una terminal, un receptor y emisor, cuando se inicia la conexión, el servicio verifica que las dos entidades sean auténticas, se asegura que la conexión no pueda ser interferida por un tercer individuo que pueda enmascararse como una de las dos entidades legítimas con el propósito de realizar una transmisión o recepción no autorizada.

6) DISPONIBILIDAD

Ocurre cuando las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario.

Para proporcionar estos servicios de seguridad es necesario incorporar *mecanismos de seguridad*.

1.6 MECANISMOS DE SEGURIDAD

Un mecanismo de seguridad es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.

Los mecanismos de seguridad implementan varios servicios básicos de seguridad o combinaciones de éstos, los servicios de seguridad especifican qué controles son requeridos y los mecanismos de seguridad especifican cómo deben ser ejecutados estos controles. Es decir, los mecanismos de seguridad son el conjunto de controles que permiten implementar un servicio de seguridad para así disminuir las vulnerabilidades de los activos.

No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información.

Los mecanismos de seguridad se pueden clasificar en general en dos categorías:

a) Mecanismos de seguridad generalizados. Se relacionan directamente con los niveles de seguridad requeridos y permiten determinar el grado de seguridad del sistema ya que se aplican a éste para cumplir la política general.

b) Mecanismos de seguridad específicos. Definen la implementación de servicios concretos.

De manera particular, por las acciones que realizan se clasifican en:

- Controles disuasivos: reducen la probabilidad de un ataque deliberado.
- Controles preventivos: protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.
- Controles correctivos reducen el efecto de un ataque.
- Controles detectores: descubren ataques y disparan controles preventivos o correctivos.

Para hacer frente a las amenazas a la seguridad del sistema se define una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información y estos servicios a su vez, hacen uso de uno o varios mecanismos de seguridad.

Se ha visto que una estrategia de seguridad, lineamientos para su gestión y mecanismos de seguridad son bases primordiales para la protección de la información, sin embargo, se requiere dirigir estos esfuerzos de manera ordenada es decir, se necesita una administración de la seguridad.

Los controles pueden ser: herramientas (físicas o lógicas). Por ejemplo: buenas prácticas, estándares o recomendaciones.

1.7 PLAN DE CONTINGENCIAS

Es necesario definir un plan de recuperación de desastres para cuando falle el sistema.

Este plan se le conoce como plan de contingencias, el cual tiene como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Debido a que se pueden presentar diferentes niveles de daños sean internos o externos, también es necesario presuponer que el daño ha sido total, con la finalidad de tener un plan de contingencias lo más completo y global posible. Los planes de contingencias se deben hacer considerando futuros acontecimientos.

La pregunta a resolver es, ¿Qué se debe realizar cuándo se presenta un problema?

Un plan de contingencias consiste en los pasos que se deben seguir después de un desastre para recuperar la capacidad funcional del sistema, para permitir que una organización continúe sus

actividades ante cualquier eventualidad presentada. La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada.

El plan de contingencias es el encargado de sostener el modelo de seguridad informática planteado y de levantarlo cuando se vea afectado.

Los responsables de la planificación deben evaluar constantemente los planes creados, deberán pensar en otras situaciones que se pudiesen producir. Un plan de contingencia estático se queda rápidamente obsoleto y alimenta una falsa sensación de seguridad, sólo mediante la revisión y actualización periódicas de lo dispuesto en el plan las medidas adoptadas seguirán siendo apropiadas y pertinentes. Toda planificación de contingencias debe establecer objetivos estratégicos, así como un plan de acción para alcanzar dichos objetivos.

Para ello es necesario establecer una planificación de las contingencias y un plan de objetivos.

- La planificación de las contingencias implica trabajar con hipótesis y desarrollar los escenarios sobre los que se va a basar la planificación.
- La planificación de objetivos conoce el punto de partida y se basará en la evaluación de las necesidades y recursos.

Toda planificación debe tener en cuenta al personal que participa directamente en ella desde el personal que lo planifica hasta aquellos que operativamente participarían en el accidente. Se deben considerar los procedimientos para la revisión del plan, quién lo actualizará y cómo esa información llegará a los afectados.

Un plan de contingencias debe ser exhaustivo pero sin entrar en demasiados detalles, debe ser de fácil lectura y cómodo de actualizar. Se debe tomar en cuenta que un plan de contingencias, debe ser operativo y debe expresar claramente lo que hay que hacer, por quién y cuándo.

Los procedimientos que componen un plan de contingencias son los siguientes:

1) Preventivos

Los procedimientos preventivos son todas aquellas actividades que se van a realizar para prevenir algo. Es decir, se planea antes de que suceda el desastre. Por ejemplo:

a) Inventario de sistemas

   Disponer de forma actualizada la situación de la infraestructura de equipos y sistemas, así como aplicaciones instaladas. Es importante para conocer cuál era la situación de cada equipo.

b) Análisis de riesgos y clasificación

   En este apartado se identificarán los riesgos y además se realizará la clasificación de las mismas. Es importante destacar que será necesario elegir un criterio de selección ya sea

por salvaguarda de la confidencialidad o integridad o disponibilidad. Después se determinará la frecuencia con que puede ocurrir. Cada cuánto se da el problema. Toda esta información se analizará decidiendo la clasificación de los riesgos según su trascendencia en la organización.

c) Asignación de responsabilidades

En definitiva delimitar y conocer a las personas implicadas y sus responsabilidades en el plan de actuación. Así como suministradores de equipamiento y servicios que puedan aunar conjuntamente esfuerzos. En este caso, disponer de contratos de mantenimiento adecuados con terceras empresas especializadas en seguridad podría significar una gran diferencia del éxito de la contingencia. También se determina como fundamental el equipo de crisis con capacidad de decisión y responsabilidad que pueda ser capaz de asumir y redirigir los problemas que se puedan dar durante la crisis.

d) Calendario de Implantación

Conocer cuál es el programa en el tiempo y poder valorar adecuadamente el momento en que se encuentre la puesta en marcha del plan.

e) Plan de pruebas y simulaciones

Por último, indicar que un buen plan de contingencias conlleva la realización periódica de pruebas y simulaciones de crisis. Sólo conociendo de antemano qué problemas podrían aparecer ante un desastre, el plan de contingencias podrá ser perfeccionado o sustituido y así asegurar el éxito del mismo.

2) Correctivos

Los procedimientos correctivos son las actividades que se van a realizar después de que el desastre surgió es decir, cómo se va a resolver ya que sucedió el desastre. Por ejemplo:

a) Plan de mantenimiento

Tanto preventivo como correctivo. Se trata por un lado de garantizar el correcto funcionamiento de los sistemas, estableciendo un calendario periódico de actuación y por otro lado, el correctivo, en el que se dispone de una guía con los fallos y las acciones a realizar para la pronta disposición del sistema.

b) Instalación de herramientas de seguridad como antivirus, antimalware, antispam, etc., así mismo la actualización de la base de datos de las herramientas.

c) Correctivo programado o planeado

Este tipo de procedimiento supone la corrección de la falla; se cuenta con el personal, las herramientas, la información y los materiales necesarios. Además al realizar la reparación

se adapta a las necesidades de la organización. Se tiene tiempo para reaccionar y no es agresivo al realizar las modificaciones.

d) Correctivo no programado o no planeado

Este tipo de procedimiento, supone la solución a la falla inmediatamente después de presentarse. Como se descubre la falla en el momento no se puede contar con todas las herramientas necesarias para corregir los errores. No se tiene la misma respuesta inmediata si es sorpresiva la falla. Este procedimiento es una situación indeseable desde el punto de vista de la producción y los ingresos.

Las características que debe tener un plan de contingencias son las siguientes:

- Responder a las necesidades particulares de la organización (auténtico).
- Factible.
- Debe involucrar a los departamentos requeridos.
- Se debe presentar por escrito.
- Debe tener el apoyo por escrito autorizado por los mandos superiores de la administración.
- Se debe actualizar constantemente.
- Ser probado.
- Se debe divulgar al personal autorizado.

Se debe presentar en forma:

- Clara y concisa.
- Modular: que facilite su elaboración, evaluación y actualización.
- Esquemática.
- De vocabulario sencillo.
- Adaptable y flexible.
- Con cubiertas de material de color llamativo, esto para poder diferenciarlo del resto de los manuales.

La función principal de un plan de contingencias es la continuidad de las operaciones de la empresa, su elaboración se divide en cuatro etapas.

- Planear.
- Hacer.
- Verificar.
- Actuar.

Las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro. Para entender estos conceptos, a continuación se explicarán las etapas de la elaboración de un plan de contingencias (ciclo PDCA/Plan-Do-Check-Act.). (Figura 1.14)

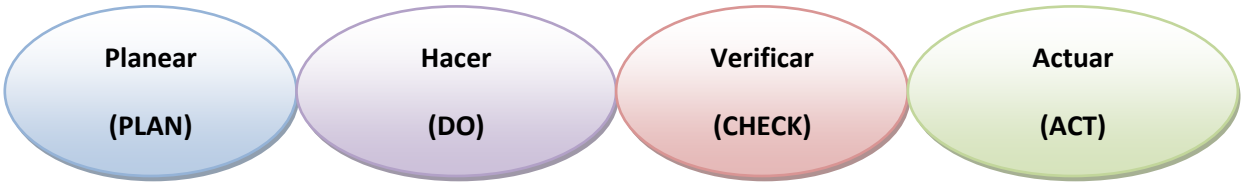

Figura 1.14 Etapas de la elaboración de un plan de contingencia

El ciclo PDCA, también conocido como "Círculo de Gabo", es una estrategia de mejora continua de la calidad en cuatro pasos. Es muy utilizado por los Sistemas de Gestión de Calidad (SGC).

El ciclo planear-hacer-revisar-actuar (plan-do-check-act PDCA) es un modelo conocido para el mejoramiento continuo de procesos. Enseña a las organizaciones a planear una acción, hacerla, revisarla para ver cómo se conforma al plan y actuar en lo que se ha aprendido.

El ciclo permite realizar un análisis de la revisión del plan de contingencias. Lo relevante de este ciclo es que es muy útil para identificar los errores o fallas en la organización ya que primero se establecen los procesos que se pretende mejorar (PLAN) para después ejecutar esos procesos (DO), ya pasado un periodo de tiempo se monitorean esos procesos y se realiza una evaluación (CHECK), al final realizar un análisis de los procedimientos utilizados y verificar si es adecuado su funcionamiento y con base en eso mejorar al procedimiento o continuar monitoreándolo.

Para tener un concepto más preciso, a continuación se detallarán las características del ciclo PDCA:

a) PLAN (Planificar)

Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora. Por ejemplo:

- Identificar el proceso que se quiere mejorar.
- Recopilar datos para profundizar en el conocimiento del proceso.
- Análisis e interpretación de los datos.
- Establecer los objetivos de mejora.
- Detallar las especificaciones de los resultados esperados.
- Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones.

b) DO (Hacer)

Implementar los nuevos procesos. Si es posible, en una pequeña escala. Por ejemplo:

- Ejecutar los procesos definidos en el paso anterior.
- Documentar las acciones realizadas.

c) CHECK (Verificar)

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora.
- Monitorea la implementación y evalúa el plan de ejecución documentando las conclusiones.

d) ACT (Actuar)

Con base en las conclusiones del paso anterior elegir una opción:

- Si se han detectado errores parciales en el paso anterior, realizar un nuevo ciclo PDCA con nuevas mejoras.
- Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos.
- Si se han detectado errores insalvables, abandonar las modificaciones de los procesos.
- Ofrece una retro-alimentación y/o mejora en la planificación.

El ciclo PDCA sirve de guía para mejorar los procedimientos que se tienen en la organización. Su función de cierto modo es prevenir y retroalimentar a la organización. Para analizar y evaluar si se está haciendo un trabajo correcto, para bien de la organización es necesario realizar una auditoría.

1.8 GESTIÓN DE SEGURIDAD

Los problemas de seguridad propician distintas acciones, por ejemplo:

- Los altos niveles de la empresa tienen que apoyar y patrocinar las iniciativas de seguridad.
- Las políticas y mecanismos de seguridad deben exigirse para toda la empresa.
- La seguridad depende de todos y cada uno de los que forman parte de la organización.

Para contrarrestar estos problemas se deben implementar un conjunto de herramientas y procedimientos destinados a proteger la tríada de la información. En pocas palabras, se debe contar con estrategias de seguridad.

Los pasos básicos para implementar una exitosa estrategia de seguridad de la información en la organización son los siguientes (Figura 1.15):

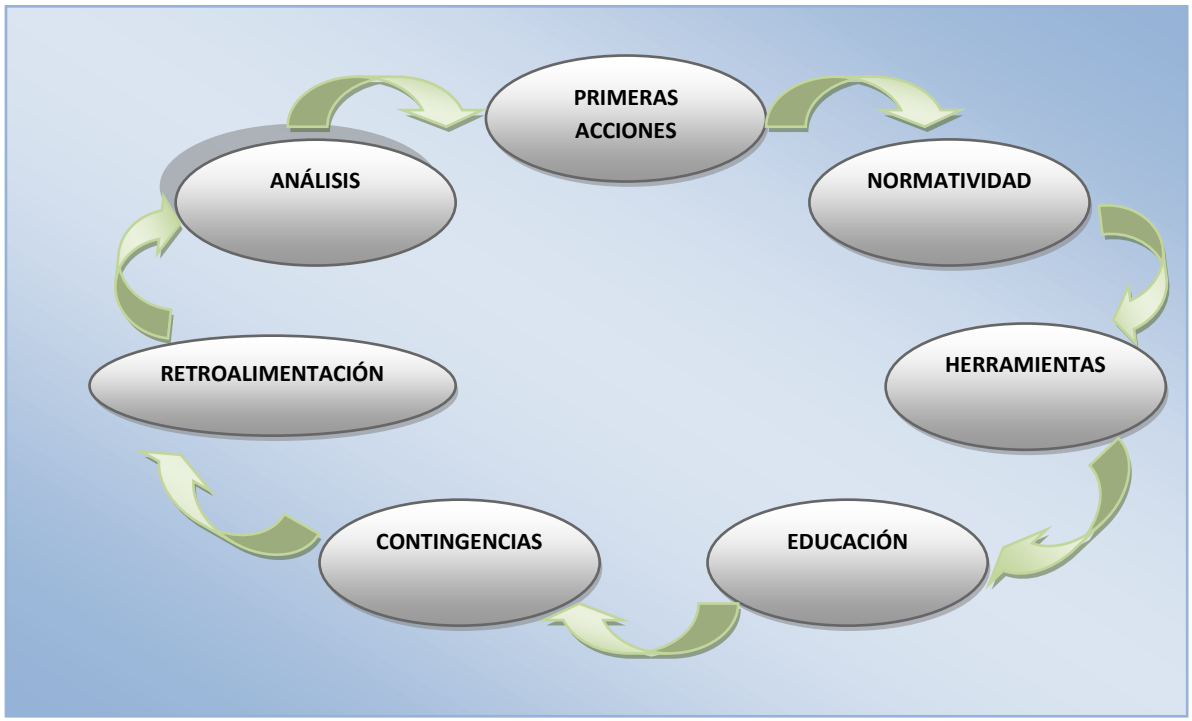

Figura 1.15 Pasos para implementar una estrategia de seguridad

1. Análisis

   Lo primero que se debe hacer en la organización es conocer el nivel de seguridad que se tiene. Es necesario realizar un diagnóstico de la madurez, a todos los niveles, sobre las prácticas y conciencia de la seguridad antes de evaluar si cumplen o no con los estándares.

   Posteriormente, se deben realizar los análisis de riesgos y vulnerabilidades. Esto consiste en hacer un diagnóstico de los componentes de la organización, desde aplicaciones e infraestructura tecnológica crítica hasta procesos de negocio y el personal, de esta manera se conoce a lo que se está expuesto y cuál será su impacto en la operación.

2. Primeras acciones

   El objetivo es determinar cuáles riesgos pueden tolerarse o transferirse y cuáles deben evitarse o mitigarse. Se debe definir el periodo de tiempo para actuar: corto, mediano o largo plazo.

   Una vez que se conocen los riesgos y se ha evaluado su impacto y el costo de disminuirlos, lo aconsejable es investigar la efectividad de los controles disponibles en el mercado para adquirir la herramienta más eficaz para controlar los riesgos más altos.

3. Normatividad

   En esta etapa se deben corregir las vulnerabilidades. Una vez hecho esto, el paso siguiente es implantar controles preventivos en los mismos. En esta etapa es el momento de desarrollar la normatividad: políticas, estándares, guías, procedimientos, procesos, controles operacionales que deberán conformar el programa de seguridad.

   En este paso se define qué se puede hacer y qué no, quién tiene acceso a qué. Lo anterior se deberá difundir en forma resumida a toda la organización. Por supuesto, deberán definirse con anterioridad los lineamientos organizacionales o corporativos, pues sobre ellos deben estar basadas las políticas. Conviene establecer amonestaciones o sanciones, cuando no se cumpla la normatividad.

4. Herramientas

   Concluidos los pasos anteriores, viene la fase de implantación de soluciones tecnológicas, como firewalls, detectores y prevención de intrusos, aplicaciones de monitoreo, entre otros. Si la organización ya cuenta con los equipos y aplicaciones, será necesario montar la estrategia sobre la infraestructura existente y hacer las adecuaciones necesarias.

5. Educación

   Puesto que el problema de la inseguridad está condicionado en buena medida por la gente, toda estrategia debe acompañarse de una campaña de seguridad. Esta estrategia puede consistir en pláticas, cursos acerca del rol de los empleados en la estrategia de protección y las responsabilidades de cada uno, así como sobre las políticas, guías, entre otros.

6. Contingencias

   Las organizaciones deben definir cómo garantizar la continuidad de sus servicios en el menor tiempo posible, incluyendo en su estrategia planes de continuidad y de recuperación de desastres. Estos planes deben incluir respuesta a sucesos que van desde el robo o pérdida de información hasta incidentes como fallas eléctricas o sismos que inhabiliten, temporal o permanentemente, el inmueble o la infraestructura.

7. Retroalimentación

   Constantemente debe verificarse cuán bien está funcionando la estrategia implementada, para hacer los cambios necesarios. Los diagnósticos o evaluaciones deberán ser continuos, dado que las organizaciones crecen o adquieren nuevos activos.

A su vez debe contemplarse una gestión de la seguridad de la información con la cual se buscará proteger la información de un amplio rango de amenazas para garantizar la continuidad, reducir riesgos y maximizar el retorno de inversión y las oportunidades de un centro de Tecnologías de la Información (TI).

Los lineamientos para una adecuada gestión de la seguridad consideran lo siguiente:

a) Seguridad organizacional.

   Coordinación y administración de la seguridad, determinar a los responsables de la seguridad, procesamiento de la información, asesoría, identificación de riesgos, requerimientos de seguridad al interior de la organización y para proveedores de servicios de outsourcing.

b) Control y clasificación de activos.

   Inventario, lineamientos, manejo y etiquetación de la información.

c) Seguridad personal.

   Acuerdos de confidencialidad, términos y condiciones de contratación, políticas, responsabilidades, capacitación o entrenamiento.

d) Seguridad física y ambiental.

   Controles, seguridad perimetral, condiciones y vigilancia de las instalaciones, seguridad de los equipos, fuentes de poder, instalaciones de cableado.

e) Administración de las operaciones y comunicaciones.

   Controles, procedimientos de manejo de incidentes, separación de responsabilidades, protección contra software malicioso, respaldos, administración de la red, seguridad en dispositivos de almacenamiento, procedimientos de manejo de la información, acuerdos de intercambio de software e información, seguridad en el correo electrónico, disponibilidad de los sistemas.

f) Control de accesos.

   Políticas de control, registro, identificación de usuarios, manejo de privilegios y contraseñas, autenticación, seguridad den los servicios de red, cómputo móvil, trabajo remoto, restricciones de acceso a la información.

g) Desarrollo y mantenimiento de sistemas.

   Requerimientos, control de procesamiento interno, autenticación de mensajes, cifrado, manejo de llaves, procedimientos de control de cambios, desarrollo de software por outsourcing.

h) Administración de la continuidad del servicio o negocio.

   Análisis del impacto y la continuidad del servicio o negocio, redacción e implantación de un plan de continuidad, pruebas, mantenimiento y evaluación del plan.

i) Cumplimiento.

Identificación de las leyes aplicables, protección de los derechos de autor, protección de los datos y privacidad de la información personal, cumplimiento de políticas, controles de auditoría de sistemas.

El problema de la seguridad informática está en su gestión y no en las tecnologías disponibles. Por lo que la seguridad informática es 80% administrador y 20% herramientas.

La solución a algunos problemas son actividades sencillas pero constantes, son las que evitan la mayoría de los problemas. Se debe trabajar en crear mecanismos de seguridad que usan las técnicas de seguridad adecuadas según lo que se quiera proteger.

1.9 AUDITORÍA

La auditoría debe estar encaminada a un objetivo específico que es evaluar la eficiencia y eficacia con que se está operando para que por medio de sus señalamientos, de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores o bien mejorar la forma de actuación.

La auditoría es una necesidad en las organizaciones, es de vital importancia para mantener el buen funcionamiento de los sistemas y la protección de los datos gestionados por esos sistemas. La auditoría se define principalmente por dos aspectos, la eficiencia y la eficacia.

La eficiencia se refiere a optimizar recursos para alcanzar objetivos. La eficacia se refiere a realizarlo en el tiempo solicitado.

Se pueden identificar diferentes tipos de auditoría respecto a las actividades de la organización. En computación las auditorías más relevantes de la seguridad son:

1) AUDITORÍA INFORMÁTICA

La auditoría informática es un examen crítico que se realiza con el fin de evaluar la eficiencia de una empresa al nivel de las TI.

La informática hoy está integrada en la gestión de la empresa y por eso las normas y estándares propiamente informáticos deben estar sometidos a los generales de la misma.

Los objetivos de la auditoría informática son:

- El control de la función informática.
- El análisis de la eficacia del sistema informático.
- La verificación de la implantación de normatividades.
- La revisión de la gestión de los recursos informáticos.

Es necesario definir el entorno y los límites donde se va a desarrollar la auditoría, es decir, el alcance. De igual forma se deben contemplar los objetivos de la misma.

En un centro de cómputo, es necesario conocer la importancia de realizar una auditoría informática.

Los aspectos importantes para realizar la auditoría informática son los siguientes:

- Para dar seguimiento a la estrategia de gestión de las TI adoptadas por la organización, es necesario continuar con el ciclo de vida de la seguridad.

- Si los objetivos de la organización no coinciden con los de la informática, es decir, síntomas de descoordinación y desorganización.

- Síntomas de mala imagen e insatisfacción de los usuarios. No se atienden solicitudes adecuadamente, errores en las aplicaciones continuamente.

- Síntomas de debilidad económica financiera. Costos y plazos de nuevos proyectos, justificaciones de inversiones informáticas.

- Síntomas de inseguridad. Evaluación de nivel de riesgos, planes de contingencias, continuidad del servicio.

2) AUDITORÍA DE SISTEMAS

La auditoría de sistemas tiene como objetivo realizar un examen de evaluación de las actividades del área de procesamiento y de la utilización de los recursos que en ellos intervienen para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas informáticos en una organización y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.

3) AUDITORÍA DE SEGURIDAD

Con una auditoría en seguridad se da una visión objetiva del nivel de exposición de los sistemas y redes a nivel de seguridad.

En la auditoría se verifica la seguridad en la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información tratada por los sistemas. Los objetivos de una auditoría de seguridad son:

- Evaluar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de políticas.
- Identificar el compromiso de equipos por parte de intrusos o software malicioso.
- Elaboración de un informe para evaluar y de ser necesario modificar las políticas. Debe incluir recomendaciones y conclusiones.

A continuación se presenta una metodología para una auditoría de seguridad, sus fases son las siguientes:

a) Definir el alcance de la auditoría: Análisis inicial y Plan de auditoría.

b) Recopilación de información: Identificación y realización de pruebas de auditoría, incluyendo si se acuerda acciones de hacking ético o análisis de vulnerabilidades en aplicaciones.
c) Análisis de las evidencias. Documentación de los resultados obtenidos, posibles pruebas de laboratorio.
d) Informe de auditoría. Informe sobre las acciones realizadas y las deficiencias detectadas. Incluir resumen ejecutivo.
e) Plan de Mejora o Recomendaciones. Propuestas para subsanar las incidencias de seguridad encontradas y mantener en el futuro una situación estable y segura de los Sistemas de Información.

Obteniendo las fases de la metodología anterior se continúa desarrollando la auditoría de seguridad:

1. Al inicio se debe definir claramente cuáles serán los objetivos de la auditoría, se solicitarán los documentos que se requieren para la realización de la misma.
2. Basado en los objetivos y documentos disponibles se crea un perfil de la organización y se genera un plan de la auditoría.
3. Basados en el plan de auditoría, se realiza una revisión de la documentación existente, en coordinación con el personal de la organización.
4. Se inicia el análisis en sitio, participando activamente con el personal involucrado, se realizan entrevistas, se inspeccionan los sites, se hace una evaluación preliminar del desempeño.
5. La información recabada durante el análisis en sitio es consolidada y examinada detenidamente.
6. Los resultados de la auditoría se resumen en un reporte final, el cual es entregado a la organización auditada.

Para llevar a cabo correctamente este desarrollo se necesitan conocer las técnicas para lograr los objetivos. Por mencionar algunas técnicas para obtener información, se tienen las siguientes:

- Entrevistas (Cuestionarios).
- Inspecciones visuales de sistemas, sitios de trabajo, sites y otros objetos en general.
- Observación (incidentes observados durante la realización de la auditoría).
- Análisis de archivos (incluyendo información electrónica).
- Análisis técnico. (Aplicaciones, sistemas de control de acceso, configuraciones, etcétera).
- Análisis de datos (bitácoras, bases de datos).

1.10 PRINCIPALES ACTORES

En el centro de cómputo se necesitan conocer los parámetros de la seguridad y al personal involucrado. Para llevar a cabo una mejor administración, se detallan las diferentes características del personal en el centro de cómputo.

1) DESARROLLADORES DE SOFTWARE

Un desarrollador de software es un programador que se dedica a realizar programas o aplicaciones en uno o varios lenguajes de programación informática; asimismo realiza proyectos referidos a la ingeniería del software. Esta persona puede contribuir a la visión general del proyecto más a nivel de aplicación que a nivel de componentes o en las tareas de programación individuales. Los desarrolladores de software suelen estar aún guiados por programadores líderes, pero también abundan los programadores independientes.

Generalmente los profesionales que se dedican al desarrollo de software son ingenieros informáticos, ingenieros de software, licenciados en ciencias de la computación, ingenieros de computación, etcétera.

Puede encontrarse una separación entre programadores y desarrolladores, siendo éstos últimos los que diseñan la estructura o jerarquía de clases. Incluso esos desarrolladores se convierten en arquitectos de sistemas informáticos, aquellos que diseñan la arquitectura a varios niveles o las interacciones entre componentes de un proyecto de software grande.

2) ALTOS EJECUTIVOS, DIRECTORES

Las funciones de los altos ejecutivos, presidentes, vicepresidentes y directores están limitadas y controladas por las complejas estructuras de la propiedad corporativa. Por su posición en la corporación tienen la posibilidad de influir de manera importante tanto en la vida y desarrollo de la corporación, como en el entorno social, económico y político de la misma.

Constituyen un grupo relativamente pequeño de personas que tienen el control efectivo sobre los recursos humanos, financieros, tecnológicos y de mercado en la corporación. Los altos ejecutivos corporativos, idealmente, son individuos que se identifican plenamente con los intereses de la organización y que han ascendido por su capacidad para servir a estos intereses. Es decir, su posición y poder dentro de la organización descansa principalmente en su eficiencia en la reproducción de la corporación y en su lealtad a la misma.

Un recurso importante de los ejecutivos son sus relaciones sociales, lo que generalmente se relaciona con su origen social.

Con frecuencia, en la mayoría de las empresas se incorporan medidas de seguridad hasta que se tienen grandes problemas. Cabe señalar que los altos ejecutivos también deben respetar esas medidas de seguridad.

3) ADMINISTRADORES DE LA RED

Un administrador de red debe mantener y desarrollar la infraestructura de red. El administrador de red debe poder controlar la actividad en la red y llamar a los técnicos rápidamente en caso de congestión o problemas de acceso. Debe poseer conocimiento preciso de todos los equipos de red, de los diferentes protocolos de comunicación, del

modelo OSI y de diferentes arquitecturas de redes. También está a cargo de administrar las cuentas de los usuarios, de crear cuentas para nuevos miembros del personal y eliminarlas cuando éstos ya no pertenecen a la compañía. El administrador de red debe estar permanentemente atento y mantener actualizados sus conocimientos sobre los últimos avances para poder modernizar la infraestructura de red de la compañía.

Actividades de los administradores de la red:

a) Los administradores de la red tienen directamente las responsabilidades de vigilar los otros roles (aparte de sus sistemas).
b) Hay actividades de seguridad que deben realizar de manera rutinaria.
c) Obligados a capacitarse, investigar y proponer soluciones e implementarlas.
d) Tienen que conocer los campos del enemigo, es decir, tienen que ser hackers para proponer soluciones inteligentes y creativas para problemas complejos.

4) USUARIO FINAL

- Los usuarios se acostumbran a usar la tecnología sin saber cómo funciona o de los riesgos que pueden correr.
- Son las principales víctimas.
- Son el punto de entrada de muchos de los problemas crónicos.
- “Es el eslabón más débil” en la cadena de seguridad.

Se tienen dos enfoques para el usuario final:

1) Principio del menor privilegio posible. Reducir la capacidad de acción del usuario sobre sistemas. Su objetivo es lograr el menor daño posible en caso de incidentes.

2) Capacitar al usuario. Generar una cultura de seguridad. El usuario ayuda a reforzar y aplicar los mecanismos de seguridad y aplicaciones. Su objetivo es reducir el número de incidentes.

CAPÍTULO 2

TIPOS DE SEGURIDAD

Es necesario considerar la administración del centro de cómputo, así como las actividades que realizan los principales actores, para brindar mejor seguridad dentro y fuera del centro de cómputo, para esto es conveniente conocer los diferentes tipos de seguridad en informática que se implementarán.

2.1 SEGURIDAD INFORMÁTICA

Son todas las herramientas informáticas que permiten brindar la protección a la información o los datos (lógicos o impresos); buscando la confidencialidad, disponibilidad e integridad.

Es necesario saber que la seguridad informática no es un problema exclusivo de las computadoras. Algunas de las razones que se deben conocer para brindar seguridad en el centro de cómputo son las siguientes:

- Las computadoras y las redes son el principal campo de batalla.
- Se debe de proteger aquello que tenga un valor para alguien.

La seguridad informática es el conjunto de herramientas y procedimientos destinados a proteger la confidencialidad, disponibilidad e integridad de la información.

Los problemas de la seguridad surgen por:

- Crecimiento exponencial de las redes y usuarios interconectados.
- Profusión de las base de datos on-line.
- Inmadurez de las nuevas tecnologías.
- Alta disponibilidad de herramientas automatizadas de ataques.
- Nuevas técnicas de ataque distribuido.
- Técnicas de ingeniería social.

Las organizaciones son cada vez más dependientes de sus sistemas y servicios de información, esto es, que son más vulnerables a las amenazas concernientes a su seguridad.

Por mencionar algunas amenazas de la seguridad informática:

- Accidentes (averías catástrofes, interrupciones).
- Errores (uso, diseño, control).
- Intenciones presenciales (atentado con acceso físico no autorizado).
- Intencionales remotas.
- Intercepción.
- Corrupción o destrucción.
- Suplantación de origen.

La solución a algunos problemas son actividades sencillas pero constantes que evitan la mayoría de los problemas.
Se debe trabajar en crear mecanismos de seguridad que usan las técnicas de seguridad adecuadas según lo que se quiera proteger.

2.2 SEGURIDAD DE LA RED

Comúnmente el activo más importante en las organizaciones es la información de la empresa, por lo que resulta de gran interés mantener la seguridad en la red. La seguridad en la red es asegurar la información que viaja de un lugar a otro a través de un medio de transmisión, ya sea terrestre o aéreo (cable o microondas, respectivamente).

Algunos puntos que se deben tomar en cuenta para el diseño de la estrategia de seguridad de la red son:

La protección contra:

- Accesos no autorizados.
- Daño intencionado y no intencionado.
- Uso indebido de información (robo de información).
- Seguridad física y perimetral.
- Supervisión y monitoreo del flujo de la información.
- Conocimiento del flujo de la información.
- Planes de contingencia.
- Auditorías.
- Utilización de herramientas anti-malware.

Las capas de seguridad de la red garantizan que tenga a su disponibilidad la información importante que estará protegida de las diferentes amenazas. Las capas de la seguridad de la red protegen, garantizan y controlan el flujo de información: (Figura 2.1)

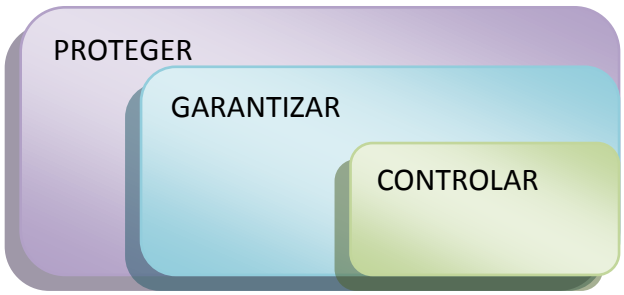

Figura 2.1 Capas de la seguridad de la red.

La utilidad de las capas de la seguridad es resguardar la información teniendo así la protección contra amenazas o ataques. A continuación se describen las distintas capas:

a) Protege contra ataques a la red tanto internos como externos.

   Las amenazas se pueden originar tanto dentro como fuera de la estructura de la empresa. Un sistema de seguridad efectivo supervisará toda la actividad de la red, detectará el comportamiento malicioso y adoptará la respuesta adecuada.

b) Garantiza la privacidad de todas las comunicaciones, en cualquier lugar y en cualquier momento.

Los empleados pueden acceder a la red desde casa o mientras se desplazan con la garantía de que sus comunicaciones serán privadas y estarán protegidas.

c) Controla el acceso a la información mediante la identificación exhaustiva de los usuarios y sus sistemas.

La empresa puede establecer sus propias reglas sobre el acceso a los datos. La denegación o la aprobación se pueden otorgar según las identidades de los usuarios, la función del trabajo u otros criterios específicos de la empresa.

Puesto que las tecnologías de seguridad permiten al sistema evitar ataques conocidos y adaptarse a las nuevas amenazas, los empleados, clientes y usuarios confiables pueden confiar en que su información estará segura.

En este momento se definen las políticas referentes a los usuarios y contraseñas que se deberán utilizar, los métodos de acceso a los servidores y a los sistemas. Se define la complejidad que deben reunir las contraseñas y la validación dentro de la red, el tiempo de trabajo de los equipos de cómputo, las áreas de acceso por cada usuario, etcétera.

El tipo de seguridad más utilizado es el basado en autentificación de usuario, el cual permite administrar y asignar derechos a los usuarios de la red. Permitiendo o denegando los accesos a los recursos a través de una base de datos en el servidor.

Para llevar un mejor control, el administrador de la red debe incluir la administración de usuarios. En caso contrario se deberá administrar mediante un grupo de usuarios, el cual da la facilidad para aplicar las políticas de seguridad a grupos específicos, es decir, a los miembros de dicho grupo.

Como medidas adicionales se deben tomar en cuenta el uso de firewall (cortafuegos) que permita administrar el acceso de usuarios de otras redes, así como el monitorear las actividades de los usuarios de la red, permitiendo así tener una bitácora de sucesos de red. Las bitácoras son de gran utilidad para aplicar auditorías a la red.

La revisión de los registros de eventos dentro de la red permite ver las actividades de los usuarios dentro de la red, esto permite al administrador darse cuenta de los accesos no autorizados por parte de los usuarios y tomar las medidas que faciliten incrementar la seguridad.

Esto puede monitorear algunas de las siguientes actividades o funciones

- Intentos de acceso.
- Conexiones y desconexiones de los recursos designados.
- Terminación de la conexión.
- Desactivación de cuentas.
- Apertura y cierre de archivos.
- Modificaciones realizadas en los archivos.
- Creación o borrado de directorios.
- Modificación de directorios.
- Eventos y modificaciones del servidor.

- Modificaciones de las contraseñas.
- Modificaciones de los parámetros de entrada.

Hay algunos organismos que certifican este tipo de software y garantizan la confidencialidad de los datos a través de la red, en especial en Internet, donde la seguridad de nuestra información es delicada.

El funcionamiento de los sistemas de cifrado funciona de la siguiente manera:

El emisor aplica el algoritmo de cifrado a los datos, éstos viajan a través de la red de tal forma que si algún intruso quiera verla no le será posible. Al llegar al destino se aplica un algoritmo inverso que permita traducir los datos a su forma original.

También se pueden implementar medidas de identificación biométrica como lectores de huella digital, escaneo de palma de mano, entre otros, esta tecnología es más segura que la simple identificación de nombre de usuario y contraseña ya que el usuario no tendrá que recordar contraseñas que en algunos casos son complejas y difíciles, además que a diferencia de las contraseñas la huella digital no se puede transferir a otros usuarios y no puede ser robada.

Además de los intrusos se tiene otro tipo de amenaza, los virus informáticos. Estos virus informáticos son pequeños programas de computadora el cual infecta equipos de cómputo y se propaga a través de la red o utilizando otros medios de transmisión como, dispositivos extraíbles, discos extraíbles.

El crecimiento de las redes y en especial de la Internet ha facilitado la propagación de virus de forma acelerada, un método de propagación de virus común es el uso de correo electrónico. Al abrir un correo infectado por virus puede infectar al equipo y puede ser capaz de reenviarse a otros usuarios de correo utilizando la libreta de direcciones del usuario.

Se debe tomar en cuenta que cualquier medio de intercambio de datos puede ser un medio potencial de propagación de virus.

Los medios más comunes pueden ser: disquetes, DVD, conexiones LAN, CD, unidades portables (memorias flash), cintas magnéticas, conexiones a Internet.

Un virus puede causar daños como pérdida de datos, evitar que el equipo arranque normalmente (daños en el sector de arranque), formateo de las unidades lógicas. Un síntoma de infección dentro de la red es que el desempeño de ésta baja considerablemente a causa de tráfico excesivo provocado por virus.

Como forma de prevención se debe considerar tener políticas contra estas amenazas que ponen en riesgo la integridad de la red. Esto se puede evitando abrir correos sospechosos, entrar en páginas de Internet con contenidos pornográficos, de juegos y páginas sospechosas. Otra forma de prevenir es instalar programas antivirus, detectores de spayware, robots, antispam, entre otras amenazas potenciales.

La seguridad en las redes se ha convertido en un factor importante en el diseño e implementación de las redes. El administrador de la red debe ser constante al implementar medidas de seguridad en la red con el fin de tener una red confiable y estable.

Aún con las medidas de seguridad que se implementen, siempre habrá amenazas en contra de las redes. Por ello es importante implementar medidas de seguridad para mitigar y reducir los tipos de amenazas.

2.3 SEGURIDAD EN LAS COMUNICACIONES

En la comunicación se transmite información de una entidad a otra. Los procesos de comunicación son interacciones, sea por medio del intercambio de opiniones, de tipo escrita u otras señales.

Todas las formas de comunicación requieren de un emisor, un mensaje y un receptor destinado. En el proceso, la información es codificada por el emisor en un paquete y canalizada hacia el receptor a través de un medio. Una vez recibido, el receptor decodifica el mensaje y proporciona una respuesta. Si se requiere tener un grado más de seguridad se necesita colocar una clave secreta para decodificar el mensaje. (Figura 2.2)

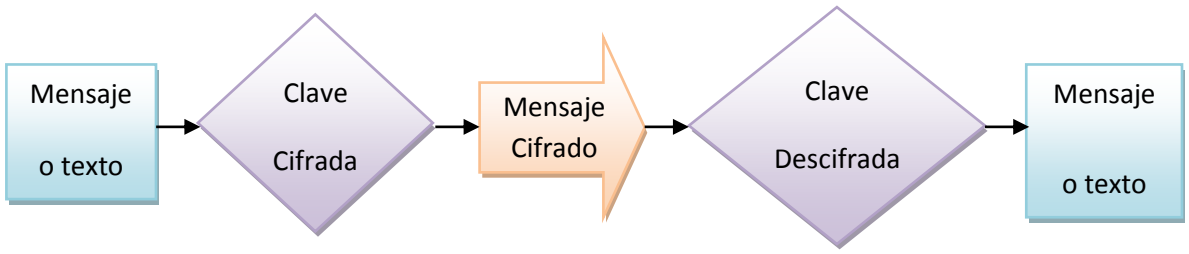

Figura 2.2 Proceso de comunicación

Se debe tener en cuenta que la clave es uno de los elementos más importantes para proteger y resguardar información. La clave no debe ser compartida con nadie, únicamente la debe conocer el emisor y receptor.

La seguridad en las comunicaciones son medidas y controles para denegar el acceso a través de las redes a entidades no autorizadas, así como para garantizar la autenticidad de las partes en comunicación. La seguridad de las comunicaciones incluye criptografía, transmisiones, emisiones y seguridad física.

En equipos de cómputo, las comunicaciones son de dos tipos: alámbrico e inalámbrico.

La comunicación alámbrica establece una conexión por medio de cables, dependiendo de las características de la comunicación el tipo de cable será distinto. A continuación se mencionan los tipos de cables que se utilizan para establecer una comunicación:

1) Cable de pares o de par trenzado: Está formado por dos hilos de cobre recubiertos cada uno de ellos por un aislante. Los cables se trenzan uno alrededor del otro para evitar que se separen físicamente. Es el cable más simple y barato que se emplea en las comunicaciones aunque su velocidad para la transmisión de datos es inferior a la que se obtiene con otros soportes y en ocasiones producen interferencias (ruidos). (Figura 2.3)

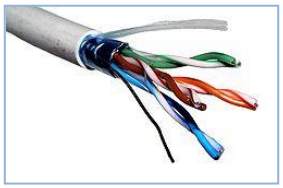

Figura 2.3 Cable par trenzado.

2) Cable coaxial: está formado por dos conductores: uno central de cobre y de sección tubular revestido por una capa de aislante (este conductor es el que realmente transmite la señal) y otro en forma de malla que rodea al aislante del primero. Este segundo conductor es una especie de toma a tierra que evita interferencias electromagnéticas. Todo el conjunto se aísla exteriormente por medio de un segundo aislante. (Figura 2.4)

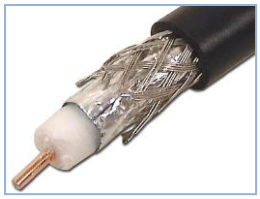

Figura 2.4 Cable coaxial.

3) Cable de fibra óptica: está formado por un núcleo central de plástico o vidrio por el que circula la luz, normalmente ultravioleta, gracias a las propiedades de reflexión de la luz. Este núcleo está revestido por varias capas de aislante y permite la transmisión de grandes cantidades de información a grandes distancias y a gran velocidad sin interferencias. (Figura 2.5)

Figura 2.5 Cable de fibra óptica.

4) Cable mixto fibra-coaxial: se emplea aprovechando instalaciones de televisión por cable y proporciona un ancho de banda importante. (Figura 2.6)

Figura 2.6 Cable mixto fibra-coaxial.

La comunicación inalámbrica no emplea cables para la transmisión de información sino que emplea ondas electromagnéticas que se pueden propagar por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión para transmitir información entre los dispositivos.

En la comunicación que se determine en el centro de cómputo, sea alámbrica y/o inalámbrica; se deben establecer los controles que se llevarán a cabo. Esto definirá la calidad de construcción, para proporcionar un desempeño, una operatividad y calidad en los sistemas de cómputo.

Algunos de los controles que se deben seguir son:

1. Instalar y actualizar las conexiones de acuerdo con las regulaciones y estándares ya establecidos.
2. Revisar previamente dónde se instalará el centro de cómputo para revisar si no hay amenazas o vulnerabilidades que puedan ser explotadas por un atacante.
3. Controles que permiten la manipulación o falsificación de registros por usuarios.
4. Realizar las conexiones de forma segura por medio de la autentificación, entre otras.
5. Controlar el acceso al centro de cómputo.
6. Detección de redes.
7. Detección de intrusos.
8. Realizar periódicamente el monitoreo de la red.
9. Instalar antivirus.
10. Instalar antispyware.
11. Instalar antimalware.
12. Realizar actualizaciones periódicamente del sistema y antivirus.
13. Realizar actualizaciones de paquetería.
14. Mantenerse informado de las anomalías en sistemas.
15. Revisar casualmente los equipos de cómputo.

2.4 SEGURIDAD INALÁMBRICA

Una red inalámbrica es donde dos o más terminales (por ejemplo, equipos de cómputo, equipos portátiles, agendas electrónicas) se pueden comunicar sin la necesidad de una conexión por cable.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya sea que se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables

ni de instalar porta cables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

Puesto que en las redes inalámbricas el medio de transmisión es el aéreo (aire), el cual es un factor de seguridad crítico. La seguridad de este tipo de redes se ha basado en la implantación de la autentificación del punto de acceso y los clientes con tarjetas inalámbricas permitiendo o denegando los accesos a los recursos de la red.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo), este tipo de red permite que los dispositivos remotos se conecten sin dificultad ya sea que se encuentren a metros o kilómetros de distancia.

Al ser una red la cual su medio de transmisión es el aire, ésta se transmite por ondas electromagnéticas, las cuales son propensas a interferencias, por esto se necesitan regulaciones que definan rangos de frecuencia y la potencia de transmisión para cada categoría. Con este motivo, un intruso puede con facilidad escuchar una red si los datos que se transmiten no están codificados, por esto se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

De acuerdo con su frecuencia de transmisión, el alcance y la velocidad de sus transmisiones hay diferentes tecnologías.

En resumen, la red inalámbrica se refiere a la transmisión de voz / datos sin cables. Este tipo de redes se dividen de acuerdo con su alcance en WMAN (redes de área amplia inalámbrica), WMAN (redes de área metropolitana inalámbrica), MLAN (redes de área local inalámbrica) y las WPAN (redes de área personal inalámbricas).

Las categorías de las redes inalámbricas dependen de acuerdo con el área geográfica desde que el usuario se conecta a la red, es decir, depende del área de cobertura. (Figura 2.7)

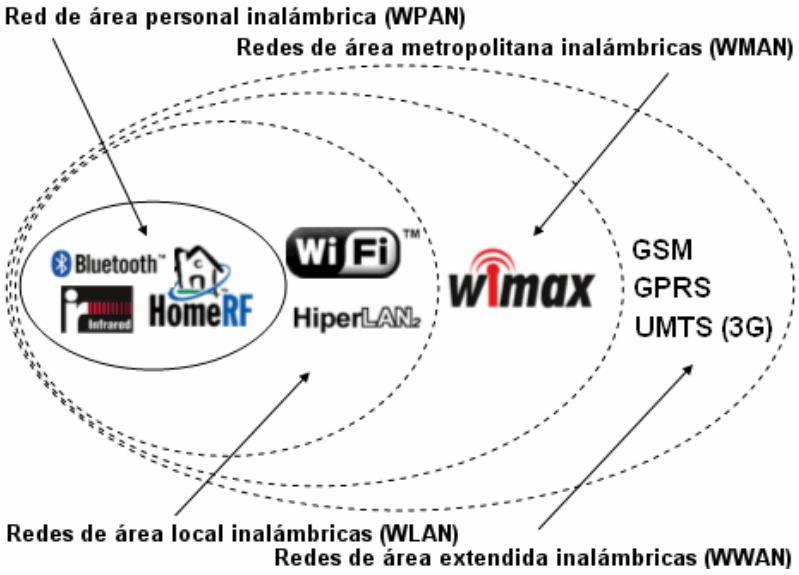

Imagen 2.7 Tipos de redes inalámbricas

Para comprender mejor estos conceptos, a continuación se explican brevemente estas categorías.

1) REDES INALÁMBRICAS DE ÁREA PERSONAL (WPAN)

Este tipo de red inalámbrica de corto alcance abarca pocos metros, esta red se utiliza para conectar dispositivos periféricos, por ejemplo, impresoras, teléfonos móviles. También para conectar un asistente personal digital (PDA) a una computadora sin conexión por cables.

Algunos ejemplos de red WPAN son las siguientes tecnologías:

La tecnología bluetooth (IEEE 802.15.1) es de bajo consumo de energía y ofrece una velocidad máxima de 1Mbps con un alcance máximo de 30 metros.

La tecnología Zigbee (IEEE 802.15.4, se puede utilizar para conectar dispositivos de manera inalámbrica con un bajo consumo de energía, se integra a pequeños aparatos como sistemas estéreos y juguetes. Ofrece una velocidad de transferencia de 250 kbps con un alcance máximo de 100 metros, cuenta con 16 canales con una banda de frecuencia de 2.4 Ghz.

Las conexiones infrarrojas se pueden utilizar para crear conexiones inalámbricas en un radio de pocos metros con velocidades que pueden alcanzar pocos megabits por segundo, esta tecnología es muy utilizada en aparatos electrónicos del hogar como controles remotos, pero tiene desventajas como sufrir interferencias debidas a las ondas de luz.

2) REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN)

Una red inalámbrica WLAN es una red que cubre un área equivalente a la red local de una organización con un alcance aproximado de 100 metros. Este tipo de red permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

Por mencionar un ejemplo de esta tecnología es WIFI (Wireless Fidelity - Fidelidad Inalámbrica). WIFI ofrece una velocidad de 54 Mbps en una distancia de varios cientos de metros. Es un protocolo de comunicación inalámbrica de área local, el estándar que define esta tecnología es el 802.11 con variantes como 802.11 a/g/e/i.

El objetivo de WiFi es fomentar las conexiones inalámbricas y facilitar la compatibilidad de los distintos equipos. Todos los productos con conectividad WiFi tienen certificada su interoperabilidad.

Hoy en día es líder en comunicación inalámbrica, esta tecnología es utilizada en aparatos como equipos portátiles, PDA, teléfonos móviles, etcétera. Desde que surgió en el año 2003 la seguridad ha supuesto un punto débil. Debido al funcionamiento de la red, se tienen que conectar los dispositivos e instalar el software correspondiente. Muchos de los enrutadores WIFI (routers WIFI) incorporan herramientas de configuración para controlar el acceso a la información que se transmite por el aire.

En la actualidad, los estándares certificados por WIFI son muy populares en todo el mundo. Este crecimiento amenaza la disponibilidad del espectro radioeléctrico, lo que aumenta el

riesgo de interferencias. Uno de los principales defectos atribuidos a la conectividad WiFi es su poca seguridad.

Al realizar conexiones inalámbricas es fácil que se intercepte la comunicación y se tenga acceso al flujo de información, por esto se recomienda el cifrado de la transmisión para emitirse en un entorno seguro.

En WIFI es posible realizar este proceso mediante protecciones como el WPA (Wi-Fi Protected Access - Acceso Wi-Fi Protegido), que es mucho más seguro que su predecesor WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado) y con nuevas características de seguridad, como la generación dinámica de la clave de acceso. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP.

Por mencionar algunas soluciones de seguridad para las redes inalámbricas se tienen las siguientes:

a) SSID (Identificador de Servicio). Protocolos de autentificación en niveles superiores.
b) Es una contraseña simple que identifica la WLAN. Cada uno de los clientes debe tener configurado el SSID correcto para acceder a la red inalámbrica.
c) Filtrado de direcciones MAC (Media Access Control - Control de Acceso al Medio).
d) Se definen tablas que contienen las direcciones MAC de los clientes que accederán a la red.
e) Adaptar la intensidad de señal en los AP (Access Points) a las necesidades.
f) WEP (Privacidad Equivalente a Cable)
g) Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.
h) WAP (Protocolo de aplicaciones inalámbricas).
i) Es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas. Por ejemplo, acceso a servicios de Internet desde un teléfono móvil.
j) Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

3) REDES INALÁMBRICAS DE ÁREA METROPOLITANA (WMAN)

Este tipo de redes WMAN también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop – Bucle Local Inalámbrico). Las redes WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad de 1 a 10 Mbps, con una distancia de 4 a 10 kilómetros.

Un ejemplo de este tipo de red es WIMAX (Worldwide Interoperability for Microwave Access - Interoperabilidad mundial para acceso por microondas), el cual puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros. El estándar que define esta tecnología es el IEEE 802.16. Una de sus ventajas es dar servicios de banda ancha en zonas

donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales). Es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2.3 a 3.5 Ghz.

Las principales características de WIMAX son:

- Distancias de hasta 80 kilómetros, con antenas muy direccionales y de alta ganancia.
- Velocidades de hasta 75 Mbps, siempre que el espectro esté completamente limpio.
- Facilidades para añadir más canales, dependiendo de la regulación de cada país.
- Anchos de banda configurables y no cerrados, sujetos a la relación de espectro.
- Permite dividir el canal de comunicación en pequeñas sub portadoras (dos tipos: guardias y datos).
- Aplicaciones para la transmisión de voz, video y datos.

WiMAX está relacionado con la seguridad, ofreciendo una protección más sólida mediante el cifrado basado en certificados. Este sistema proporciona servicios de voz, vídeo y datos, con calidad de servicio independiente.

Los sistemas WiMAX aseguran la privacidad de usuarios finales y previene el acceso a información confidencial.

Esta seguridad se tiene en los terminales, ya que están asociados con una estación base y sincronizados, tanto por frecuencia y tiempo, y utilizan un protocolo riguroso para comunicarse con la unidad de acceso. La misma regla se aplica para un dispositivo de intercepción para que los datos sean interceptados, un dispositivo wireless debe ser empleado y sincronizado dentro del área cubierta por la unidad de acceso.

Para estar protegido, los sistemas WiMAX necesitan aplicar medidas para asegurar la privacidad de sus usuarios finales y prevenir del acceso a información confidencial o sensible a personas que no están autorizadas.

La forma de prevenir que los intrusos no intercepten información sensible y confidencial es que los usuarios tengan en cuenta que su sistema es privado y seguro, que las medidas apropiadas están disponibles para minimizar los riesgos de seguridad, incluyendo:

a) Escuchas/espionaje: interceptar información de forma intencional cuando se está transmitiendo.

b) Privacidad: Asegurarse de que la información transmitida es solamente leída por los destinatarios a los que va dirigida.

c) MAC Spoofing: evitar que un atacante copie las direcciones MAC de CPE legítimas con el fin de conseguir el acceso a la red.

d) Robo del Servicio: prevenir que los agresores puedan acceder a Internet u otros servicios utilizando CPE (Equipo Local del Cliente) robadas. El CPE es un equipo de telecomunicaciones usado en interiores como en exteriores para originar, encaminar o terminar una comunicación.) .

e) Adquirir servicios de forma gratuita, sea paquetería o sistema.

Para prevenir el uso indebido de la conexión wireless se debe cifrar la clave. La seguridad WIMAX soporta dos estándares de cifrado de calidad, TDES y AES.

- TDES (Triple Data Encryption Standard – Estándar de cifrado de Datos Triple). Método para cifrar la información, para agrandar la clave. Es utilizada en la mayoría de las tarjetas de crédito y otros medios de pago electrónicos.
- AES (Advanced Encryption Standard – Estándar de cifrado Avanzada). Es más rápido que el TDES, no se ha encontrado vulnerabilidad.

4) RED INALÁMBRICA DE ÁREA EXTENSA (WWAN)

Este tipo de redes WWAN tienen el alcance más amplio de todas las redes inalámbricas. Es por ello que todos los teléfonos móviles están conectados a una red inalámbrica de área extensa.

Las principales tecnologías de este tipo de red son:

- GSM (Global System for Mobile Communication – Sistema Global para las comunicaciones Móviles)
- GPRS (General Packet Radio Service - Paquetes de datos de servicio móvil)
- UMTS (Universal Mobile Telecommunication System – Sistema Universal de Telecomunicaciones Móviles)

Las redes de área extensa inalámbrica WWAN se emplean para conectarse a Internet a través de un móvil o celular. Este tipo de red tiene:

- Una rápida comunicación entre computadoras y conectividad con Internet y otras redes externas.
- Una fácil comunicación entre oficinas que se encuentran en lugares separados.
- Acceso seguro a la red de la compañía desde un lugar remoto.

WWAN, también denominada red "3G" o "4G", es una opción de banda ancha portátil que cubre un área amplia. Se puede usar en cualquier lugar donde tenga cobertura. Exige un servicio celular proporcionado por un operador, por lo que hay que pagar una suscripción mensual.

La seguridad en este tipo de red:

- Brinda cobertura inalámbrica regional, nacional y global.
- Brinda mayor seguridad, debido al cifrado incorporado.
- Emplea tecnología celular para proteger la transferencia de datos o la conexión a Internet.
- Debido a que el contrato se realiza con el proveedor, es más costoso. El uso de este servicio es controlado por el proveedor y por el usuario.

En la actualidad las redes inalámbricas están en constante crecimiento, esto representa un reto para los administradores que tienen que desarrollar medidas más eficaces para mantener seguras las redes.

2.5 SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET

Internet es un protocolo, un estándar, un acuerdo que define un método simple, fiable y aplicable a múltiples plataformas heterogéneas para el transporte de datos entre distintos equipos de cómputo. Se denomina Internet al conjunto de redes interconectadas y abiertas al público, que funcionan con este protocolo. La red que hoy en día se conoce como Internet, es una red de redes, esparcidas por todo el mundo.

La World Wide Web (WWW) es un sistema de hipertexto que opera sobre la Internet. Para ver la información en él contenida, uno debe utilizar un software, un navegador o browser para ver las páginas web desde los servidores o sitios web.

La evolución y el acceso a Internet en estos últimos tiempos ha crecido enormemente y hoy hay mucha gente, especialmente las nuevas generaciones ya nacieron con esta tecnología, por lo que dentro de un tiempo, el Internet será algo intrínseco en la vida, y su crecimiento no se podrá detener.

Ahora bien, similar a la dependencia del teléfono celular, el Internet ha hecho que muchas cosas se mejoren, haciendo procesos más eficientes, búsquedas de información mucho más sencilla, comunicación a distancia en tiempo real y especialmente que ha economizado mucho los costos de los envíos de mensajes que anteriormente sólo se daba por correspondencia.

Pero también ha traído muchas cosas malas, como toda tecnología lo hace, y es hacer que las personas sean mucho más cómodas, trabajen menos y accesibles a otro tipo de información desagradable.

Por lo que a continuación se listan algunas ventajas y desventajas del Internet en estos últimos tiempos.

Ventajas:

- Hace la comunicación mucho más sencilla.
- Es posible conocer e interactuar con muchas personas de todas partes del mundo.
- La búsqueda de información se vuelve mucho más sencilla, sin tener que ir forzadamente a las bibliotecas tradicionales.
- Es posible encontrar muchos puntos de vista diferentes sobre alguna noticia.
- Es posible la creación y descarga de software libre por sus herramientas colaborativas.
- La computadora se actualiza periódicamente más fácil que si no se tuviera Internet.
- Es posible encontrar soporte técnico de toda clase sobre alguna herramienta o proceso.

- El seguimiento de la información en tiempo real es posible a través de Internet.
- Es posible compartir muchas cosas personales o conocimientos que a otro le puede servir, y de esa manera, se vuelve provechoso.

Desventajas:

- Así como es fácil encontrar información buena, es posible encontrar de la misma forma información mala, desagradable (pornografía, violencia explícita, terrorismo) que puede afectar especialmente a los menores.
- Genera una gran dependencia o vicio de internet, descuidando muchas cosas personales o laborales.
- Hace que los estudiantes se esfuercen menos en hacer sus tareas, debido a la mala práctica del copy/paste (copiar/pegar).
- El principal puente de la piratería es internet (música, videos, etcétera.)
- Distrae a los empleados en su trabajo.
- Dependencia de procesos. Si hay un corte de internet, hay muchos procesos que se quedan varados por esa dependencia.
- Dependencia de energía eléctrica. Si hay un corte de energía en la casa, adiós internet (no es el caso de la telefonía convencional).
- Hace que nazcan otros males tales como el spam, el malware, la proliferación de los virus, el phising, etcétera.

Así como todo, hay cosas buenas y cosas malas, así que hay que saber equilibrar el uso de internet para que sea adecuado en la vida.

A continuación se muestran los riesgos y las recomendaciones para proteger los datos en Internet.

a) Riesgos sociales

En este tipo de riesgo la adicción a Internet es muy alta en aspectos de pornografía o videojuegos, música, pero también se puede sufrir difamación, estafas, engaños, acoso y cadenas. Los niños están expuestos a riesgos como pornografía infantil, secuestro o cyberbullying (ciberacoso). Este último, se entiende como el uso de información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles, y websites difamatorios para acosar a un individuo o grupo, mediante ataques personales u otros medios.

La mejor manera de prevenir es moderando el tiempo y los contenidos que se visitan; no compartir información personal o de la familia a desconocidos y enseñar esto a los hijos; activar funciones de control de padres para monitorear el uso que los niños hacen de Internet.
Los niños son los más vulnerables, por lo que es importante tener control sobre ellos, debe

ayudárseles a elegir un alias que no revele nada personal ni sea sugestivo. Es recomendable realizar una lista de seguridad para ellos y colocarla cerca del equipo.

b) Riesgos informáticos

El sistema de correo electrónico o E-mail permite el envío de mensajes de texto y archivos entre usuarios, de modo similar a como funciona un apartado postal en la vida real. Fue el primer servicio ampliamente utilizado en Internet. Actualmente es el servicio empleado por más usuarios de Internet.

La computadora y la información que contiene están constantemente amenazadas de robo. Virus, gusanos o troyanos pueden infectar equipos, pero existe también el SPAM, spyware, adware, malware, phishing, pharming y más de mil amenazas detectadas que habitan en línea.

El phising es un fraude en el que se roba información a partir del engaño, principalmente ocurre en portales bancarios falsos, donde el usuario accede a una liga enviada a su correo con alguna supuesta notificación del banco.

Por ejemplo: ¡Su tarjeta ha sido bloqueada! Siga esta liga para solucionar el problema. El usuario atiende e ingresa datos personales al supuesto portal bancario sin percatarse que voluntariamente ha entregado a ladrones las credenciales necesarias para realizar acciones ilícitas.

La manera de prevenir este problema es Ingresar siempre al portal tecleando la dirección completa y revisar que mientras se permanezca en él, conserve el nombre en la barra de direcciones, si se aprecia que el sitio cambia de razón es probable que sea fraudulento.

Los navegadores actuales incluyen dispositivos de seguridad automáticos como un candado o el color de la barra que puede ser verde o blanco para un sitio seguro y rojo para uno amenazante.

c) Mecanismos de infección

Las memorias USB que pasan de una computadora a otra pueden contener malware, correo electrónico de contactos infectados, sitios de dudosa procedencia como páginas ilegales (pornografía infantil, trata de blancas), redes sociales, sobre todo aplicaciones, ligas involuntarias que se colocan en muros, redes p2p para descargas ilegales de contenidos (música, libros) y software pirata.

Para prevenir esto se debe cuidar los sitios que se visitan, identificar correos o ligas de dudosa procedencia y no instalar software pirata. Los portales que ofertan decir “quién ha visitado su perfil en Facebook” o los “contactos que le han eliminado del Messenger” son portadores de malware.

P2P (peer-to-peer - par a par- o de punto a punto)

A grandes rasgos, esta tecnología es una red informática entre iguales, se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan

simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es una forma de compartir archivos de forma similar a cómo se hace en el email o mensajeros instantáneos, sólo que de una forma más eficiente.

Este modelo de red contrasta con el modelo cliente-servidor, el cual se rige mediante una arquitectura monolítica donde no hay distribución de tareas entre sí, sólo una simple comunicación entre un usuario y una terminal, en la que el cliente y el servidor no pueden cambiar de roles.

Las redes de P2P, son redes que aprovechan, administran y optimizan el uso de banda ancha que acumulan de los demás usuarios en una red por medio de la conectividad entre los mismos usuarios participantes de la red, obteniendo como resultado mucho más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total de banda ancha y recursos compartidos para un servicio o aplicación. Comúnmente, estas redes se conectan en gran parte con otros nodos vía "ad hoc" (es una red inalámbrica descentralizada, donde cada nodo está preparado para reenviar datos a los demás).

Dichas redes son útiles para muchos propósitos, pero se usan frecuentemente para compartir toda clase de archivos que contienen: audio, video, texto, software y datos en cualquier formato digital. Este tipo de red es también comúnmente usado en telefonía VoIP para hacer más eficiente la transmisión de datos en tiempo real, así como lograr una mejor distribución del tráfico de la telefonía utilizando tecnología P2P.

Cualquier nodo puede iniciar, detener o completar una transacción compatible. La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local (cortafuegos, NAT, ruteadores, etcétera.), velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco.

Se debe contar con controles de seguridad para cada nodo, utilizar cortafuegos, antivirus, antimalware. Realizar el escaneo periódico del sistema. Antes de enviar cualquier tipo de información corroborar con la herramienta adecuada que no tenga virus para que no se comprometa el servicio.

d) Elección de contraseñas

Al ingresar al sistema, al correo electrónico, red social, cuenta bancaria, etcétera. Se necesita utilizar una contraseña robusta que proporcione seguridad ya que de no ser así se tiene el riesgo que un atacante la conozca fácilmente, utilizando las herramientas indicadas. Por ejemplo: involucrando ingeniería social, forma diccionario, fuerza bruta, etcétera.

La mala elección de contraseñas es un riesgo para el usuario y para la organización ya que se puede perder información sensible.

Por ello al elegir una contraseña segura, ayuda a mantener la identidad de cada usuario a salvo en Internet. Se recomienda utilizar una combinación de letras mayúsculas, minúsculas,

números y símbolos. Es importante no colocar nombres obvios, como fechas de nacimiento, gustos, es decir, algo peculiar que se relacione con el usuario.

La mayoría de los usuarios de Internet utilizan contraseñas débiles y fáciles de adivinar, convirtiéndose en una presa fácil para los delincuentes informáticos. Un ejemplo de esto son los recientes ataques a LinkedIn donde salió a la luz las contraseñas más repetidas en la red, por ejemplo:

1. Password
2. 123456
3. Football
4. 696969
5. qwerty
6. Abc123
7. 111111
8. Mustang

Listando algunos consejos para elegir una contraseña segura se tiene:

- No colocar la misma contraseña para todas las cuentas.
- Todas las contraseña deben incluir mayúsculas, minúsculas y números.
- Deberán tener al menos entre 8 y 12 caracteres.
- No seleccionar la casilla que dice recordar usuario y/o contraseña.
- Cambiar la contraseña con regularidad.
- No usar información personal, así como: fechas importantes o nombre de algún familiar.
- No divulgar a nadie la contraseña.

Además de la elección de contraseñas seguras se recomienda utilizar un firewall, esto para:

- Mantener actualizado el sistema operativo y las aplicaciones (no usar software pirata).
- Instalar, actualizar y mantener actualizaciones en antivirus.
- Instalar, actualizar y mantener activo el antispyware.

Un firewall en Internet es un sistema de seguridad que impone una política de seguridad entre la organización de red privada y el Internet. (Figura 2.8)

Figura 2.8 Sistema de Firewall de Seguridad

Determina los servicios de red que puede entrar para utilizar los recursos de red pertenecientes a la organización. El tráfico de información a través del Internet pasa por el firewall para examinar la información. Este sistema no puede ofrecer protección, una vez que el agresor lo traspasa o permanece en torno a éste. Algunos beneficios de utilizar un firewall en Internet son:

- Administrar los accesos posibles del Internet a la red privada.
- Mantener al margen usuarios no autorizados fuera de la red, prohibiendo la entrada o salida al vulnerar los servicios de la red.
- Proporcionar protección para posibles ataques.
- Simplificar los trabajos de administración, al distribuirse en cada servidor de la red privada.

2.6 SEGURIDAD FÍSICA

La seguridad física se comprende la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos e información.

Uno de los principales objetivos de este tipo de seguridad es proteger contra elementos de la naturaleza y contra errores humanos.

Con este tipo de seguridad se disminuyen riesgos, se considera que se obtiene un trabajo mejor ya que se mantiene la sensación de seguridad. Además de que se cuenta con los medios para luchar contra accidentes.

Las consideraciones que se deben tener en un centro de cómputo para el área de las computadoras, en distintos aspectos, por ejemplo, en el caso de incendio, no deben estar cerca de fábricas con equipos flamables. No se debe fumar en esta área, debe haber pisos falsos para colocar el cableado, además de colocar cestos metálicos para los papeles, entre otras cosas.

Algunos aspectos para evitar inundaciones, son tratar de que el centro de cómputo esté en el segundo piso o que tenga una mayor cantidad de ventanillas de ventilación.

Para evitar terremotos, si se cuenta con la posibilidad se deben construir edificios considerando la ubicación, el tipo de suelo y la zona en que se va a ubicar.

Respecto a las instalaciones eléctricas, en una organización se debe tener solo una línea regulada para el centro de cómputo y para la energía del edificio. De preferencia, si se cuenta con el presupuesto colocar plantas de energía.

Para llevar a cabo la seguridad física, es necesario tomar en cuenta las herramientas para la administración de la seguridad. A continuación se describen:

2.6.1 REVISIÓN DE PERÍMETRO

Una de las principales actividades de la seguridad informática es proteger el perímetro de la red en la organización, para tener una adecuada confianza en los sistemas del interior del perímetro. El perímetro de red es toda la frontera de área local. Sin embargo, actualmente el perímetro es

cualquier lugar donde los sistemas de confianza se encuentran con el tráfico de red desconfiable. Se conoce como perímetro de red como la porción o porciones de red de una organización que están directamente conectadas a Internet.

Algunos elementos del perímetro son los siguientes:

a) Routers de frontera

El router se encarga de dirigir el tráfico interno y externo de la red. El router de frontera es el último dispositivo bajo el control que distingue la red interna de las redes inseguras como el Internet. Comúnmente el router es un dispositivo de seguridad, el cual se utiliza como la primera capa de protección en una arquitectura de seguridad general y a veces en las redes pequeñas se utiliza un firewall. La implementación más común de un router en una arquitectura de seguridad es como dispositivo de análisis.

b) Firewalls

Un firewall es un dispositivo que tiene un conjunto de reglas específicas, con las cuales determina qué tráfico de red entra o sale de la red. Generalmente es usado para interconectar una red privada con Internet, también se utiliza para implementar controles de acceso al interior de la red. Normalmente un firewall está ubicado en la frontera de ésta.

Hay tres tecnologías de firewall:

1) Filtrado de paquetes (Packet Filter)

   Se basa en permitir o denegar el tráfico de red basado en el encabezado de cada paquete. No guarda los estados de una conexión, no tiene sesiones.

2) Filtrado por estado (Stateful Application Inspection)

   Permite abrir puertas a determinado tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina. Este tipo de filtrado mantiene un registro de las conexiones, las sesiones y su contexto.

3) Filtrado por aplicación (Full Application Inspection)

   Es capaz de inspeccionar hasta el nivel de aplicación. No sólo la validez de la conexión sino todo el contenido de la trama. Es considerado el más seguro. Este tipo de filtrado soporta la autenticación a nivel de usuario.

c) Sistemas Detectores de Intrusos (IDS)

Este tipo de sistema detecta tráfico malicioso en la red. Un IDS escucha el tráfico de manera promiscua, monitorea los paquetes en la red y alerta si hay una actividad maliciosa. Además es capaz de detectar gran cantidad de tipos de ataques. Requiere de una excesiva administración y soporte.

Los IDS tienen dos categorías principales, los que son basados en host (HIDS) y de red (NIDS).

Los HIDS residen y protegen un host, mientras que los basados en red residen en uno o más hosts dedicados en exclusiva a la investigación de la red, el cual protege a todos los hosts conectados a la misma. Por ejemplo: open source, AIDE, Tripware.

Los NIDS monitorean el tráfico de la red en busca de actividades sospechosas. Algunos de estos sistemas residen de subredes y están directamente conectados al firewall, así como a los puntos críticos en la red interna. Por ejemplo: Snort, Firestorm, Prelude.

d) Sistemas Preventores de Intrusos (IPS)

Este sistema bloquea tráfico malicioso durante el mismo flujo de la información. Forma parte de la estructura de la red. Disminuye la actividad administrativa para su mantenimiento.

Algunas diferencias entre un IDS y un IPS son:

- IDS. No están en la red, si se quita el IDS, el flujo de la red continúa.
- IPS. Están en la red, si se quita el IPS no hay flujo de red.

e) Redes Privadas Virtuales (VPN)

Esta red es virtual porque conecta dos redes físicas (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden ver los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

El funcionamiento de una VPN es el siguiente:

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro. (Figura 2.9)

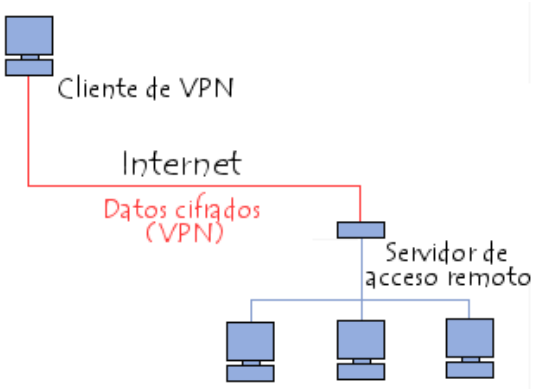

Figura 2.9 Red privada virtual

En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

f) Zonas Desmilitarizadas

Una zona desmilitarizada (conocida también como DMZ o red perimetral) es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuego, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). (Figura 2.10)

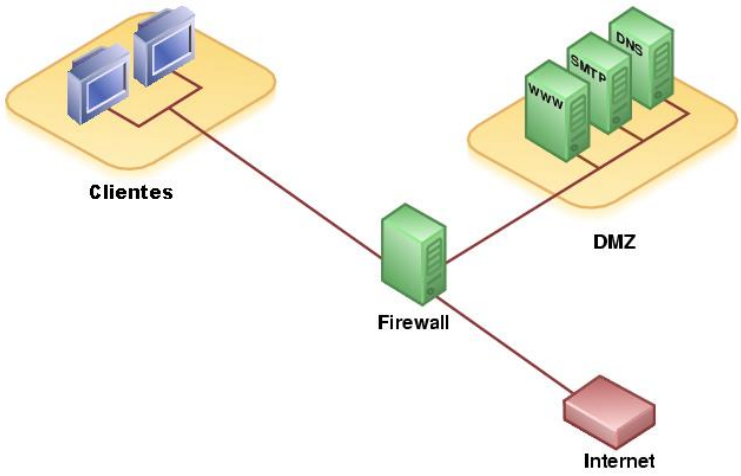

Figura 2.10 Red típica que usa una DMZ con un cortafuegos de tres patas (three-legged).

g) Arquitectura de Software

La arquitectura del software es el diseño de más alto nivel de la estructura de un sistema. Una arquitectura de software se selecciona y diseña con base en objetivos y restricciones. Los objetivos son aquellos prefijados para el sistema de información, pero no solamente los de tipo funcional, también otros objetivos como la mantenibilidad, auditabilidad, flexibilidad e interacción con otros sistemas de información.

Las restricciones son aquellas limitaciones derivadas de las tecnologías disponibles para implementar sistemas de información. Unas arquitecturas son más recomendables de implementar con ciertas tecnologías mientras que otras no son aptas para determinadas arquitecturas.

La arquitectura de software define, de manera abstracta, los componentes que llevan a cabo alguna tarea de computación, sus interfaces y la comunicación entre ellos. Toda arquitectura debe ser implementable en una arquitectura física, que consiste en determinar qué computadora tendrá asignada cada tarea.

La arquitectura de software, tiene que ver con el diseño y la implementación de estructuras de software de alto nivel. Es el resultado de ensamblar un cierto número de elementos arquitectónicos de forma adecuada para satisfacer la mayor funcionalidad y requerimientos de desempeño de un sistema, así como requerimientos no funcionales, como la confiabilidad, escalabilidad, portabilidad, y disponibilidad.

Toda arquitectura de software debe describir diversos aspectos del software. Cada uno de estos aspectos se describe de una manera más comprensible si se utilizan distintos modelos o vistas. Es importante destacar que cada uno de ellos constituye una descripción parcial de una misma arquitectura.

Existen al menos tres vistas fundamentales en cualquier arquitectura:

- La visión estática: describe qué componentes tiene la arquitectura.
- La visión funcional: describe qué hace cada componente.
- La visión dinámica: describe cómo se comportan los componentes a lo largo del tiempo y cómo interactúan entre sí.

Las vistas o modelos de una arquitectura de software pueden expresarse mediante uno o varios lenguajes, por ejemplo el lenguaje natural, pero existen otros lenguajes tales como los diagramas de estado, los diagramas de flujo de datos, etcétera.

Las arquitecturas más universales son:

- Cliente-servidor. Donde el software reparte su carga de cómputo en dos partes independientes pero sin reparto claro de funciones.
- Orientada a servicios. Es un concepto de arquitectura de software que define la utilización de servicios para dar soporte a los requisitos del negocio.
- Máquinas virtuales.

2.6.2 REVISIÓN DE MONITOREO

Las redes de cómputo se vuelven cada vez más complejas y la exigencia de operación es cada vez más demandante. Las redes soportan cada vez más aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas.

El monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras en busca de componentes defectuosos o lentos para luego informar a los administradores de redes mediante correo electrónico o alarmas. Es un subconjunto de funciones de la administración de redes.

Mientras que un sistema de detección de intrusos monitorea una red por amenazas del exterior (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga o fallas en los servidores, como también problemas de la infraestructura de red u otros dispositivos.

La monitorización de redes también ayuda a optimizar la red, ya que facilita información detallada sobre el uso del ancho de banda y otros recursos de la red.

Algunas de las herramientas para monitorear la red son:

a) Nessus:

Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

b) Ethereal:

Ethereal es un analizador de protocolos de red para Unix y Windows. Permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se desee ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

c) Snort:

Snort es un sistema de detección de intrusiones de red, capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas.

d) Netcat:

La navaja multiuso para redes. Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Es una herramienta rica en características, útil para depurar y explorar, ya que puede crear casi cualquier tipo de conexión que se pueda necesitar y tiene muchas habilidades incluidas.

e) TCPDump / WinDump:

Tcpdump es un analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red que concuerden con cierta expresión de búsqueda. Se puede utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades.

f) Ettercap:

Es un interceptor/sniffer/registrador para LANs con ethernet basado en terminales. Tiene la habilidad para comprobar si en una LAN con switches y de identificar huellas de sistemas operativos para dejarnos conocer la geometría de la LAN.

g) OpenSSH / SSH:

Una manera segura de acceder a computadoras remotas. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables sobre una red insegura. También se pueden redirigir conexiones de X11 y puertos arbitrarios de TCP/IP sobre este canal seguro. La intención de esta herramienta es la de reemplazar a `rlogin', `rsh' y `rcp', y puede ser usada para proveer de `rdist', y `rsync' sobre una canal de comunicación seguro.

h) Kismet:

Un poderoso sniffer para redes inalámbricas. Kismet es un sniffer de redes 802.11b. Es capaz de husmear utilizando la mayoría de las placas inalámbricas; de detectar bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP; listar equipos de Cisco por medio del "Cisco Discovery Protocol"; registrar paquetes criptográficamente débiles y de generar archivos de registro compatibles con los de ethereal y tcpdump. También incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes.

i) Fport:

Fport reporta todos los puertos, TCP/IP y UDP abiertos en la máquina en la que es ejecutado y muestra qué aplicación abrió cada puerto y sus aplicaciones asociados.

2.6.3 EVALUACIÓN DE CONTROLES DE ACCESO

a) Identificación por huella dactilar

A este tipo de identificación también se le conoce como fingerprinting o huella dactilar. El fingerprinting se refiere a la identificación por medio de huellas digitales o de los dedos.

Son diferentes técnicas, en la que es posible identificar con mayor o menor grado de certeza, un dispositivo, host, sistema operativo, etcétera. El fingerprinting es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red.

Las técnicas de fingerprinting aplicadas a la seguridad en redes, son conocidas, documentadas y a menudo utilizadas por administradores y profesionales de la seguridad.

La identificación de sistemas operativos con base en la implementación que el mismo haya realizado de la pila TCP/IP o la forma en la que requerimientos mal formados, son respondidos, deja un rastro capaz de identificar los mismos con un alto porcentaje de fiabilidad.

A continuación se muestran algunos tipos de fingerprinting:

1) Humano
   - De identificación de huellas dactilares: Fue desarrollada por Sir Francis Galton en 1888.
   - Tipos de huellas dactilares: De patente, de plástico, y huellas latentes.
   - Clasificación de huellas dactilares.
   - Los patrones de huellas dactilares.
   - Las cuatro clasificaciones básicas son el arco, el lazo, los verticilos, y los compuestos.

2) DNA

   - Identificación de huellas dactilares de ADN: Fue desarrollado en 1985 por Sir Alec Jeffreys en Inglaterra.
   - Métodos ADN fingerprinting.

3) Servicios

   - Notario Público.
   - Notario móvil.
   - Huellas de exploración en directo.

4) Productos

   - Escáneres de huellas dactilares.
   - Cierre la puerta de huellas dactilares.
   - Cajas fuertes de huellas dactilares.
   - Almohadillas de tinta de huellas dactilares.
   - Kits de huellas dactilares.

- Polvo de huellas dactilares.

b) Código de barras

El código de barras es un código basado en la representación mediante un conjunto de líneas paralelas verticales de distinto grosor y espaciado que en su conjunto contienen una determinada información, es decir, las barras y espacios del código representan pequeñas cadenas de caracteres.

El código de barras permite reconocer rápidamente un artículo de forma única, global y no ambigua en un punto de la cadena logística y así poder realizar inventario o consultar sus características asociadas.

La correspondencia o mapeo entre la información y el código que la representa se denomina simbología. Estas simbologías pueden ser clasificadas en grupos atendiendo a dos criterios diferentes:

1) Continua o discreta: en las simbologías continuas los caracteres comienzan con un espacio y en el siguiente comienzan con una barra (o viceversa). Sin embargo, en las simbologías discretas los caracteres comienzan y terminan con barras y el espacio entre caracteres es ignorado y generalmente de poca anchura.

2) Bidimensional o multidimensional: En las simbologías bidimensionales las barras pueden ser anchas o estrechas. Sin embargo, las barras en las simbologías multidimensionales son múltiplos de una anchura determinada.

Nomenclatura del código de barras:

- Módulo: Es la unidad mínima o básica de un código. Las barras y espacios están formados por un conjunto de módulos.
- Barra: El elemento oscuro dentro del código. Se hace corresponder con el valor binario 1.
- Espacio: El elemento claro dentro del código. Se hace corresponder con el valor binario 0.
- Carácter: Formado por barras y espacios. Normalmente se corresponde con un carácter alfanumérico.

Entre las justificaciones de la implantación del código de barras se tiene la necesidad de agilizar la lectura ya sea en gafetes de identificación para llevar un control de horarios y permisos al ingresar y la forma de evitar errores de digitación. Algunas ventajas de utilizar el código de barras:

- Posee porcentajes muy bajos de error.
- Permite capturar rápidamente los datos.
- Los equipos de lectura e impresión de código de barras son flexibles y fáciles de conectar e instalar.

La información se procesa y almacena con base en un sistema digital binario donde todo se resume a sucesiones de unos y ceros. Algunos ejemplos donde se requiere la implementación del código de barras son en:

- Control de inventario.
- Control de movimiento.
- Control de acceso.
- Control de calidad.
- Rastreos preciso en actividades.
- Facturación.
- Servicio de bibliotecas.

c) Tarjeta electrónica o Tarjeta inteligente

Una tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI), permite la ejecución de cierta lógica programada.

La percepción estándar de una tarjeta inteligente es una tarjeta microprocesadora de las dimensiones de una tarjeta de crédito (o más pequeña, como por ejemplo, tarjetas SIM o GSM) con varias propiedades especiales y es capaz de proveer servicios de seguridad (por ejemplo, la confidencialidad de la información en la memoria). Las tarjetas no contienen baterías; la energía es suministrada por los lectores de tarjetas.

Según las capacidades de su chip, las tarjetas más habituales son:

1) Memoria: tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Éstas se usan generalmente en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.

2) Microprocesadas: tarjetas con una estructura análoga a la de una computadora (procesador, memoria volátil, memoria persistente). Éstas albergan ficheros y aplicaciones y suelen usarse para identificación y pago con monederos electrónicos.

3) Criptográficas: tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta (por ejemplo, sin que se instale en el almacén de certificados de un navegador web) ya que es el procesador de la propia tarjeta el que realiza la firma.

Tipos de tarjetas según la estructura de su sistema operativo:

1) Tarjetas de memoria. Tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Disponen de un sistema operativo limitado con una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria y

pueden tener capacidades de seguridad para proteger el acceso a determinadas zonas de memoria.

2) Basadas en sistemas de ficheros, aplicaciones y comandos. Estas tarjetas disponen del equivalente a un sistema de ficheros que exponen una serie de comandos que se pueden invocar a través de programación.

3) Java Cards. Una Java card es una tarjeta capaz de ejecutar mini-aplicaciones Java. En este tipo de tarjetas el sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar aplicaciones específicas para este entorno.

Las aplicaciones de las tarjetas inteligentes incluyen su uso como tarjeta de crédito, SIM para telefonía móvil, tarjetas de autorización para televisión por pago, identificación de alta seguridad, tarjetas de control de acceso y como tarjetas de pago del transporte público.

Cuando las tarjetas son criptográficas, las posibilidades de identificación y autenticación se multiplican ya que se pueden almacenar de forma segura certificados digitales o características biométricas en ficheros protegidos dentro de la tarjeta de modo que estos elementos privados nunca salgan de la tarjeta y las operaciones de autenticación se realicen a través del propio chip criptográfico de la tarjeta.

De modo más particular, las aplicaciones más habituales son:

1) Identificación digital: este tipo de aplicaciones se utilizan para validar la identidad del portador de la tarjeta en un sistema centralizado de gestión.

2) Control de acceso: este tipo de aplicaciones se utilizan para restringir o permitir el acceso a una determinada área en función de distintos parámetros que pueden estar grabados en la tarjeta o pueden ser recuperados de un sistema central de gestión a partir de la identidad grabada en la tarjeta.

3) Este tipo de aplicaciones suelen estar ligadas a puertas o tornos automatizados que permiten/impiden el paso físico de una persona a una determinada área, si bien también tiene sentido este servicio en el ámbito de la autenticación en sistemas informáticos (webs, sistemas operativos, etcétera).

4) Monedero electrónico: esta aplicación se utiliza como dinero electrónico. Se puede cargar una cierta cantidad de dinero (en terminales autorizadas que dispongan de las claves de seguridad oportunas) y luego, sobre esta cantidad de dinero se pueden realizar operaciones de débito o consulta de modo que puede ser utilizado para el pago o cobro de servicios o bienes.

5) Firma Digital: este tipo de aplicaciones permiten almacenar un certificado digital de forma segura dentro de la tarjeta y firmar con él, documentos electrónicos sin que en ningún momento el certificado (y más concretamente su clave privada) salgan del almacenamiento seguro en el que están confinados.

6) Fidelización de clientes: Este tipo de aplicación sirve a las empresas que ofrecen servicios o descuentos especiales para clientes que hacen uso de la tarjeta para poder validar la identidad del cliente, y para descentralizar la información.

7) Sistemas de Prepago: En estos sistemas, un cliente carga su tarjeta con una cierta cantidad, la cual va siendo decrementada a medida que el cliente hace uso del servicio. El servicio puede variar desde telefonía móvil hasta TV por cable, pasando por acceso a sitios web o transporte público.
8) Tarjetas sanitarias: En algunos hospitales y sistemas nacionales de salud ya se está implementando un sistema de identificación de pacientes y almacenamiento de los principales datos de la historia clínica de los mismos en tarjetas inteligentes para agilizar la atención.

En cualquier caso, todos los servicios pueden ser derivados de los tres puntos planteados inicialmente (identificación, pago y almacenamiento seguro). Como se mostró anteriormente, la seguridad es una de las propiedades más importantes de las tarjetas inteligentes y se aplica a múltiples niveles y con distintos mecanismos.

CAPÍTULO 3

ANÁLISIS DE RIESGOS

Ya que no se puede contar con una seguridad total, un análisis de riesgos sirve para identificar las consecuencias probables o los riesgos asociados con las vulnerabilidades y así implementar controles que reduzcan los efectos a un nivel aceptable.

Este procedimiento identifica los controles de seguridad existentes, calcula vulnerabilidades y evalúa el efecto de las amenazas en cada área vulnerable, en la mayoría de los casos, el análisis de riesgos intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos.

Para realizar un análisis de riesgos, primero se debe conocer que el riesgo es la posibilidad de sufrir alguna pérdida. El riesgo es una medida de la probabilidad de que una amenaza, a través de una vulnerabilidad, afecte el correcto funcionamiento de un sistema; tomando en cuenta el impacto resultante de dicho evento. (Figura 3.1)

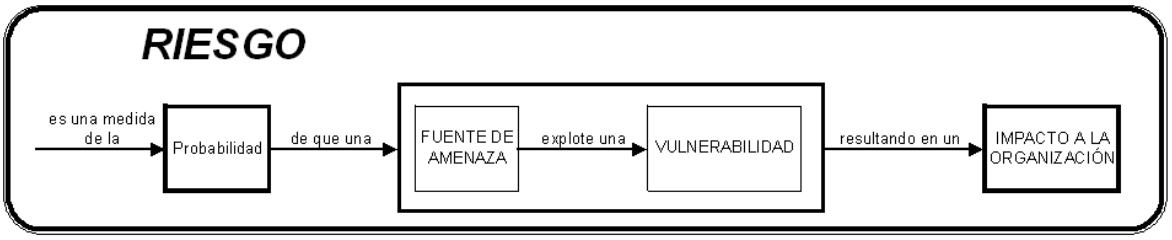

Figura 3.1 Concepto de riesgo

Según María Jaquelina López y Cintia Quezada en su libro Fundamentos de Seguridad Informática. "Un análisis del riesgo de seguridad es un procedimiento para estimar el riesgo de los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas. El procedimiento primero determina el nivel de vulnerabilidad del activo tras identificar y evaluar el efecto de los controles colocados en el lugar. Un nivel de vulnerabilidad del activo para cierta amenaza se determina con controles que se encuentran en el lugar en el momento en el que se realiza el análisis del riesgo".[9]

La intención es ser preventivo, identificar vulnerabilidades, generando estrategias de seguridad y las herramientas que se van a necesitar.

Un análisis de riesgos es importante para:

- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.
- Determinar los activos críticos.
- Efectuar un análisis de los peligros, exposiciones, debilidades y amenazas potenciales.
- Identificar, definir y revisar todos los controles de seguridad ya existentes.

[9] María Jaquelina López y Cintia Quezada. Fundamentos de seguridad informática. UNAM. Facultad de Ingeniería, 2006. Página 157

- Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.
- Reducir la probabilidad de que ocurra un evento.
- Proporcionar los elementos de seguridad para que en caso de que acontezca un desastre, éste tenga un impacto mínimo.

El proceso de análisis de riesgos es una parte del ciclo de vida de un esquema de seguridad. (Figura 3.2)

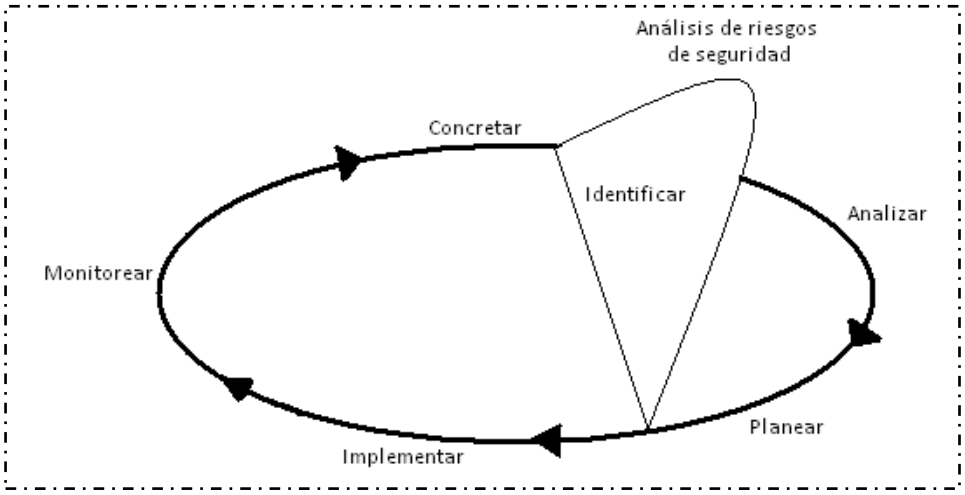

Figura 3.2 Ciclo de vida de un esquema de seguridad

3.1 TERMINOLOGÍA

En un proceso de análisis del riesgo debe considerarse la siguiente terminología:

1. Activo. Es todo aquello con valor para una organización y que necesita protección. Por ejemplo: datos, hardware, software, personal y su experiencia, información, servicios, etcétera.
2. Riesgo. Es la posibilidad de sufrir algún daño o pérdida.
3. Aceptación del riesgo. La decisión para aceptar un riesgo.
4. Análisis del riesgo. Uso sistemático de información disponible para identificar las fuentes y para estimar qué tan seguido determinados eventos no deseado pueden ocurrir y la magnitud de sus consecuencias.
5. Manejo del riesgo. Proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar sistemas de información, por un costo aceptable.
6. Evaluación del riesgo. Comparación de los resultados de un análisis del riesgo con los criterios estándares del riesgo u otros criterios de decisión.

7. Impacto. Pérdidas como resultado de la actividad de una amenaza, las pérdidas son normalmente expresadas en una o más áreas de impacto –destrucción, denegación de servicio, revelación o modificación-.
8. Pérdida esperada. El impacto anticipado y negativo a los activos debido a una manifestación de la amenaza.
9. Vulnerabilidad. Una condición de debilidad.
10. Amenaza. Acción potencial que puede suceder o existir, pero no existe aún. Con la posibilidad de causar daño.
11. Riesgo residual. El nivel de riesgo que queda después de la consideración de todas las medidas necesarias, los niveles de vulnerabilidad y las amenazas relacionadas. Éste debe ser aceptado como es o reducirse a un punto donde pueda ser aceptado.
12. Control. Son los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización. Un mismo control puede ser implementado para una o varias políticas de seguridad, lo cual indica que la relación forzosamente no es uno a uno.

Un análisis del riesgo de seguridad define el ambiente actual y realiza acciones correctivas recomendadas si el riesgo residual no es aceptable, además es de utilidad ya que identifica los puntos más débiles en un sistema. Por ello es importante identificar las relaciones de los elementos de un análisis de riesgos. (Figura 3.3)

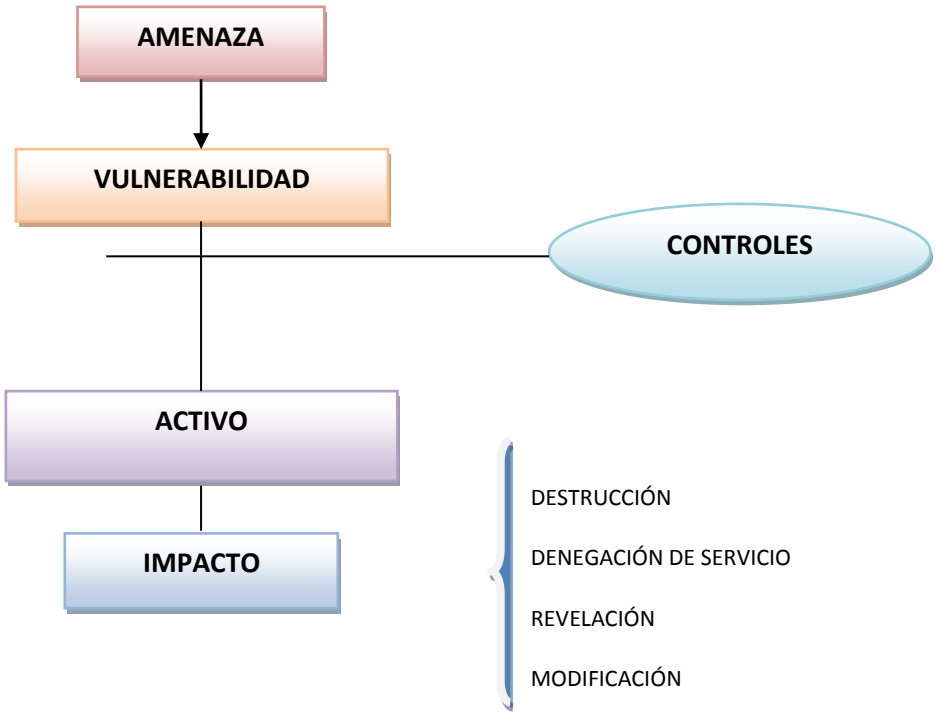

Figura 3.3 Relaciones entre los elementos de un análisis de riesgo

El objetivo del análisis del riesgo es tener la capacidad de:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguridad de la información.
- Enfocar recursos y esfuerzos en la protección de los activos

3.2 TIPOS DE ANÁLISIS DE RIESGOS

El proceso para determinar qué controles de seguridad son apropiados y rentables es una de las principales funciones del análisis del riesgo de seguridad; esto es, poner este proceso sobre una base objetiva. Hay dos tipos de análisis del riesgo.

a) Análisis cuantitativo del riesgo

Todos los activos, sus recursos y los controles se identifican y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema, de tal forma que se identifiquen las áreas que son sensibles. Con esto se puede decidir si los controles existentes son adecuados o si se requiere la implementación de otro.

Este tipo de análisis busca obtener valores numéricos, casi siempre de carácter económico de los activos que se están estudiando y su pérdida posible. Los resultados obtenidos son expresados de igual manera en porcentajes, probabilidades de ocurrencia, pesos, entre otros.

Es demasiado complicado llevarse a cabo, debido a que es muy difícil asignársele valores monetarios a la información, es decir, cuánto puede valer la información, un registro en la base de datos, los archivos de configuración, etcétera, en muchas ocasiones ni siquiera los altos mandos lo tienen claro. Sólo es sencilla la asignación de valores monetarios a los activos físicos.

b) Análisis cualitativo del riesgo

En lugar de establecer valores exactos se dan notaciones como alto, bajo, medio que representa la frecuencia de ocurrencia y el valor de los activos. Un problema en este tipo de análisis es el consenso que se debe realizar para jerarquizar la información, los controles y decidir sus valores, otra dificultad es la comparación de la pérdida potencial con el costo de implementación de controles para minimizarla, así como qué tan factible resulta aplicar los controles y en qué niveles de información.

No se requiere la asignación de valores numéricos a los activos que se encuentren en estudio. Los resultados son subjetivos, pero son basados en las interpretaciones y experiencia de los dueños de la información, ya que ellos tienen muy en claro qué tan crítica o sensible es. Los

cálculos son sencillos. La calidad de estos estudios dependerá de la objetividad con que se lleve a cabo el proceso de recopilación de información.

Ambos tipos del análisis del riesgo utilizan los siguientes elementos:

a) Amenazas. Las amenazas están siempre presentes en cada sistema.

b) Vulnerabilidades: las vulnerabilidades permiten que un sistema sea más propenso a ser atacado por una amenaza o que un ataque tenga mayor probabilidad de tener cierto éxito o impacto.

c) Controles: son medidas contra las vulnerabilidades. Hay cuatro tipos.

- Los controles disuasivos reducen la probabilidad de un ataque deliberado.
- Los controles preventivos protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.
- Los controles correctivos reducen el efecto de un ataque.
- Los controles detectores descubren ataques y disparan controles preventivos o correctivos.

A continuación se ilustran mediante un modelo relacional. (Figura 3.4)

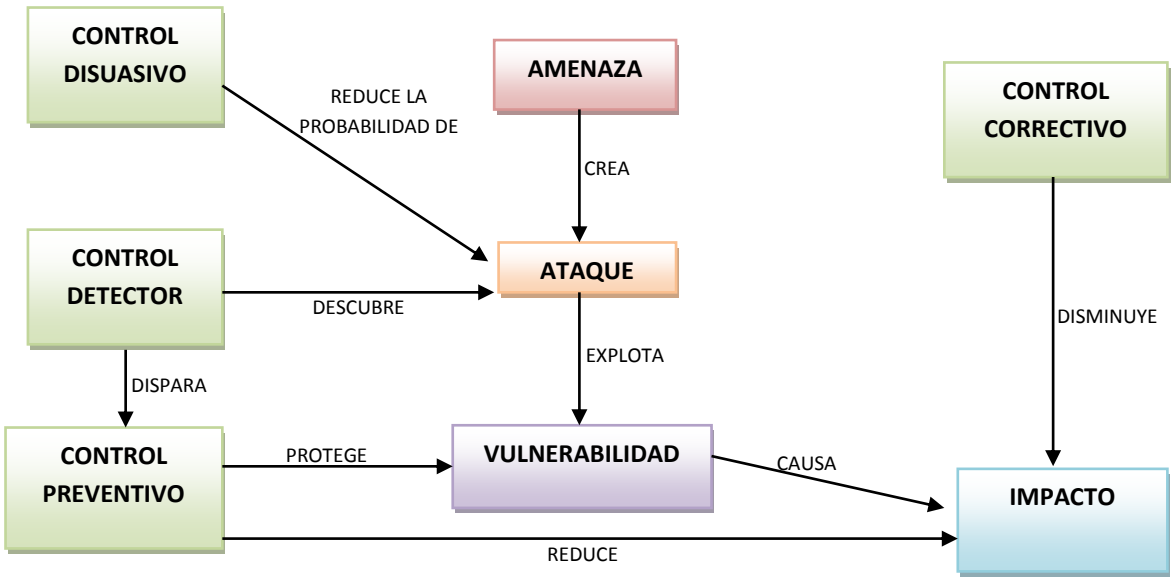

Figura 3.4 Modelo relacional simple

Cualquier análisis del riesgo de seguridad debe indicar:

- El actual nivel de riesgo.
- Las consecuencias probables.
- Qué hacer con el riesgo residual si es muy alto.

Los tres elementos principales en un análisis del riesgo son:

- Un balance del impacto o del costo de alguna dificultad específica si ésta sucede.
- Una medida de la efectividad de los controles dentro del lugar.
- Una serie de recomendaciones para corregir o minimizar los problemas identificados.

3.3 PASOS DEL ANÁLISIS DE RIESGOS

La planeación para la seguridad de la información y del manejo del riesgo empieza con la identificación de los activos de seguridad, la sensibilidad de los datos, los valores, los controles dentro del lugar, la configuración del sistema o proyecto, amenazas probables y su frecuencia de ocurrencia. Esta información es utilizada para calcular las vulnerabilidades y los riesgos. El proceso de análisis de riesgo consiste en ocho pasos. (Figura 3.5)

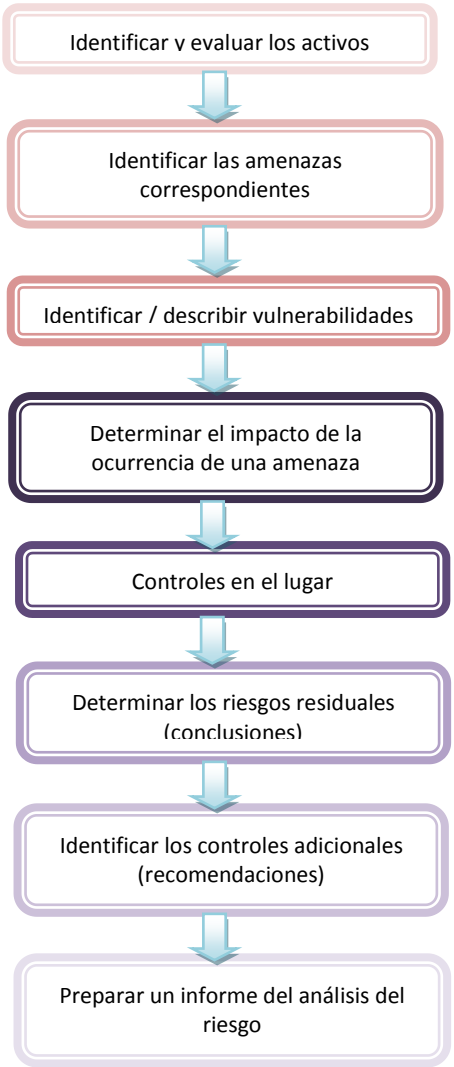

Figura 3.5 Pasos para el proceso de análisis de riesgos

A continuación se describen los pasos para el proceso de análisis del riesgo:

a) Identificar y evaluar los activos

El valor de los activos es un factor significante en la decisión para realizar cambios operacionales o para incrementar la protección de los activos. El valor del activo se basa en su costo, sensibilidad, misión crítica o la combinación de estas propiedades.

b) Identificar las amenazas correspondientes

Después de identificar los activos que requieren protección, las amenazas a éstos deben identificarse y examinarse para determinar cuál sería la pérdida si dichas amenazas se presentan. Este paso envuelve la identificación y la descripción de las amenazas correspondientes al sistema o red que está siendo utilizado y se estima qué tan seguido se puede presentar. Esto incluye el acceso no autorizado, revelación de información, denegación de servicio, puntos de acceso, desconfiguración de sistemas, amenazas internas, errores de programación en el software.

c) Identificar / describir vulnerabilidades

El nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente, aunque hay áreas de alta vulnerabilidad que no tienen consecuencia si no presentan amenazas.

d) Determinar el impacto de la ocurrencia de una amenaza

Cuando la explotación de una amenaza ocurre, los activos sufren cierto impacto. Las pérdidas son catalogadas en áreas de impacto llamadas:

- Revelación: cuando la información es procesada y se pierde la confidencialidad.
- Modificación: el efecto de la manifestación de una amenaza cambia el estado original del activo.
- Destrucción: pérdida completa del activo
- Denegación de servicio: pérdida temporal de los servicios.

e) Controles en el lugar

La identificación de los controles es parte del proceso de recolección de datos en cualquier proceso de análisis del riesgo.

- Controles requeridos: todos los controles en esta categoría pueden ser definidos con base en una o más reglas escritas. La clasificación de los datos almacenados y procesados en un sistema o red y su modo de operación determinan qué reglas aplicar, y éstas indican cuáles son los controles requeridos.

- Controles discrecionales: este tipo de controles es elegido por los administradores. En muchos casos los controles requeridos no reducen el nivel de vulnerabilidad a un nivel aceptable, por lo que se deben elegir e implementar este tipo de controles para ajustar el nivel de vulnerabilidad a un nivel aceptable.

f) Determinar los riesgos residuales (conclusiones)

Siempre existirá un riesgo residual, por lo tanto, debe determinarse cuándo el riesgo residual es aceptable o no. El riesgo residual toma la forma de las conclusiones alcanzadas en el proceso de evaluación. Las conclusiones deben identificar:

- Las áreas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de la amenaza.
- Todos los controles que no están dentro del lugar.

El resultado de estos pasos permite comenzar la selección necesaria de controles adicionales.

g) Identificar los controles adicionales (recomendaciones)

Aquí se identifica la forma más efectiva y menos costosa para reducir el riesgo a un nivel aceptable. Las recomendaciones son:

- Recomendación de controles requeridos: controles requeridos u obligatorios que no se encuentran en el lugar, son la primera recomendación.
- Recomendación de controles discrecionales: la segunda recomendación generalmente identifica los controles discrecionales necesarios para reducir el nivel de riesgo.

h) Preparar un informe del análisis del riesgo

El proceso de análisis de riesgo ayuda a identificar los activos de información en riesgo y añade un valor a los riesgos, adicionalmente identifica medidas protectoras y minimiza los efectos del riesgo y asigna un costo a cada control. El proceso de análisis del riesgo determina si los controles son efectivos o no. Se debe realizar un informe de la evaluación del riesgo, el cual debe contener:

- Niveles de vulnerabilidad.
- Amenazas correspondientes y su frecuencia.
- El ambiente usado.
- Conexión del sistema.
- Niveles o nivel de sensibilidad de los datos.
- Riesgo residual, expresado en una base individual de vulnerabilidad.
- Cálculos detallados de la expectativa de pérdida anual.

El análisis de riesgo de seguridad es fundamental en la seguridad de cualquier organización ya que es un método formal para investigar los riesgos de un sistema informático y recomendar las medidas apropiadas que deben adoptarse para controlar estos riesgos. En esencial asegurarse que los controles y el gasto que implican sean completamente proporcionales a los riesgos a los cuales se expone la organización.

Para identificar el estado de la seguridad en la organización se propone llevar a cabo el proceso de gestión de riesgos, considerar las principales metodologías para llevar a cabo la gestión de riesgos, así como el estándar a seguir. A continuación se identifican estos puntos para identificar, mitigar y corregir el riesgo.

1) GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso que muestra el estado de la seguridad al momento de la realización del estudio, ya que un sistema de TI no es estático, es decir, cambian los activos, se identifican nuevas vulnerabilidades y amenazas, motivaciones, etcétera. Por lo que habrá que realizar un nuevo estudio cada cierto tiempo o en el caso de un cambio radical en las tecnologías utilizadas.

La gestión de riegos abarca tres procesos: el análisis de riesgos, la mitigación de riesgos y el proceso de gestión y evaluación. (Figura 3.6)

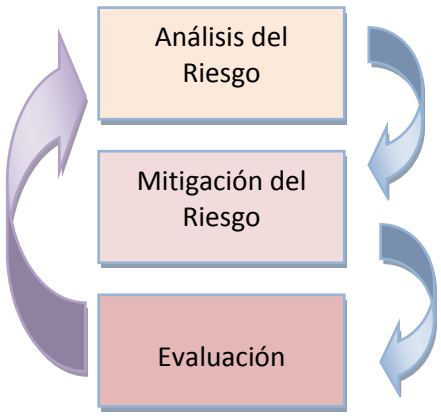

Figura 3.6 Esquema de gestión de riesgos

A continuación se describe el esquema de gestión de riesgos.

a) Análisis de riesgos

Es el proceso de identificar los riesgos de operación (incluyendo misión, visión, funciones, imagen o reputación), y los recursos de una organización o de un individuo, mediante la determinación de distintos parámetros como:

- Probabilidad de ocurrencia.
- Impacto resultante.
- Controles de seguridad que mitiguen el impacto.

Durante la evaluación de riesgos se realizan los análisis de amenazas (donde se identifican las fuentes de amenaza potenciales y sus causas) y de vulnerabilidades (mediante el cual se identifican las vulnerabilidades a las que está expuesto el sistema y las acciones que podrían ocasionarse si se llegan a explotar).

La identificación de un riesgo requiere de un entendimiento del ambiente del proceso del sistema. Las personas que realizan el análisis de riesgos previamente deben recolectar información relativa al sistema, por ejemplo:

- Hardware.
- Software.

- Interfaces del sistema (conectividad interna y externa).
- Información y datos.
- Personal que mantiene y utiliza el sistema.
- Misión del sistema.
- Nivel crítico del sistema y los datos.
- Sensitividad del sistema y los datos.
- Requerimientos funcionales del sistema.
- Usuarios.
- Políticas de seguridad del sistema a las que está sujeto.
- Arquitectura de seguridad.
- Topología de red.
- Protección y almacenamiento de la información.

Si el sistema se encuentra en fases de inicio o de diseño, la información puede derivarse de los documentos de diseño y requerimientos del mismo. Si el sistema se encuentra en desarrollo, es necesario definir reglas y atributos de seguridad planeados para su implementación en un futuro.

b) Mitigación de riesgos

Es el proceso mediante el cual los riesgos identificados en la evaluación de riesgos son abordados, buscando una disminución en el impacto potencial en la organización. Incluye un estudio de costo-beneficio, selección y evaluación de controles de seguridad y asignación de responsabilidades. Es, en sí, una estrategia que busca atenuar los riesgos.

En este proceso se prioriza, evalúa e implementan los controles recomendados resultado del proceso de evaluación de riesgos. La eliminación de un riesgo es difícil, por lo que se debe tener un acercamiento del menor costo e implementar los controles más apropiados para decrecer el riesgo hasta un nivel aceptable.

La mitigación de riesgos se podrá alcanzar mediante sólo una de las siguientes opciones:

- Aceptación del riesgo. Se acepta el riesgo potencial y se implantan controles para la reducción del riesgo a un nivel aceptable.
- Evitar el riesgo. Se evita el riesgo eliminando la causa y la consecuencia.
- Limitación del riesgo. Se limita el riesgo implantando controles que minimizan el impacto adverso de la explotación de una vulnerabilidad.
- Planeación del riesgo. Se administran los riesgos desarrollando un plan de mitigación de riesgos que prioriza, implanta y mantiene controles de seguridad.
- Investigación y reconocimiento. Se reduce el riesgo reconociendo la vulnerabilidad o falla e investigando qué controles pueden corregirla.
- Transferencia del riesgo. Se transfiere el riesgo, utilizando distintas opciones para la compensación de pérdidas, por ejemplo, la adquisición de un seguro.

Para escoger cualquiera de estas opciones, se deberá tomar en cuenta los objetivos de la misión de la organización.

c) Gestión y evaluación

En este proceso se considera que los sistemas o las redes están en continua expansión, por lo que pueden llegar a cambiar sus componentes, el software utilizado, el personal, entre otras cosas. Por lo que surgirán nuevos riesgos o algunos previamente mitigados podrán volver a ser una preocupación o incluso podrían desaparecer. Se deberá indicar la periodicidad con la que se tendrá que llevar a cabo la gestión de riesgos.

Una gestión de riesgos efectiva, deberá tener el compromiso de los directivos, el completo apoyo y participación del personal a cargo de los sistemas, la cooperación y concientización de los usuarios, que deberán seguir procedimientos y cumplir con los controles implantados y una evaluación continua.

Las claves para una gestión de riesgos exitosa son:

- Compromiso con la alta gerencia.
- Apoyo total y participación del personal.
- La eficiencia del personal de la evaluación de riesgos.

La conciencia y cooperación de los miembros de la comunidad de usuarios del sistema que deberán seguir procedimientos y cumplir con los controles implantados para garantizar el cumplimiento de la misión de la organización.

2) METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS

En la actualidad hay diferentes metodologías para la gestión de riesgos. A continuación se explicarán brevemente dos de ellas muy utilizadas:

a) OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation – Evaluación operacional crítica de amenazas, activos y vulnerabilidades).

Desarrollado por el Sofware Engineering Institute de la Universidad de Carnegie Mellon. Es una metodología de planeación y evaluación basada en riesgos. Se dice que es auto-dirigida, es decir, las personas dentro de la organización donde se aplica asumen la responsabilidad de establecer la estrategia de seguridad organizacional.

Maneja dos aspectos fundamentales, la seguridad operacional y prácticas de seguridad. Cuando OCTAVE es aplicado, las organizaciones realizan las decisiones de protección de información basándose en los riesgos que afectan la confidencialidad, integridad y disponibilidad de los recursos relacionados con los recursos que la afectan.

OCTAVE consta de tres fases: Construcción de perfiles de amenazas, identificación de las vulnerabilidades en la infraestructura, desarrollo y planeación de la estrategia de seguridad. (Figura 3.7)

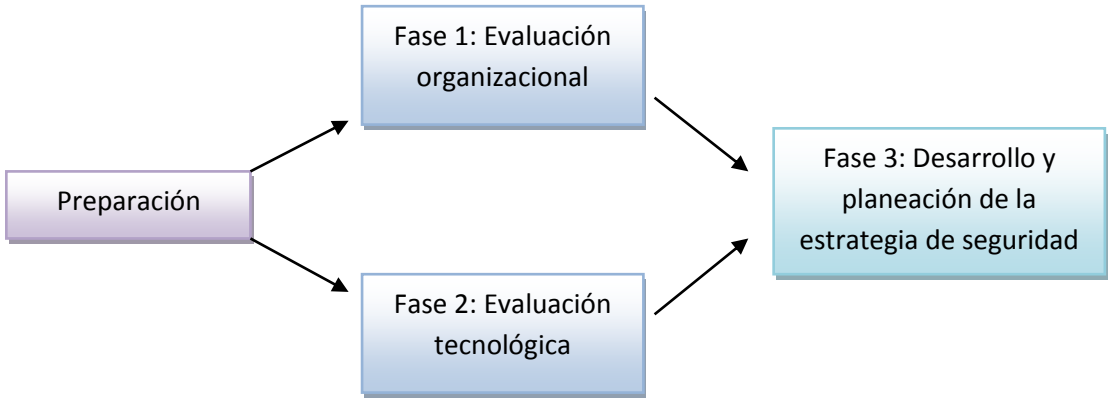

Figura 3.7 OCTAVE

b) MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

Desarrollada en Madrid. Se enfoca en el desarrollo de un proyecto de análisis y gestión de riesgos que se compone de tres grandes pasos: planificación, análisis y gestión; cada uno consta de distintas actividades que están estructuradas por diversas tareas. (Figura 3.8)

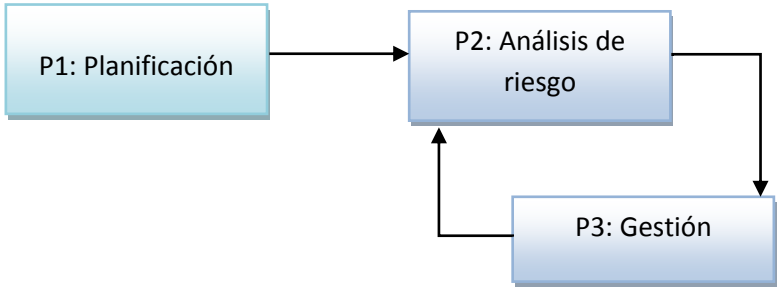

Figura 3.8 MAGERIT

3) ESTÁNDAR DE SEGURIDAD

El estándar ISO 27002 propone una serie de controles de seguridad para un sistema de gestión de la información (SGSI). Está diseñado para satisfacer los requerimientos identificados, mediante un análisis de riesgos.

Incluye 11 cláusulas de control de seguridad o secciones diseñadas para ser implantados y que satisfagan los requerimientos de seguridad identificados por una gestión de riesgos. Cada categoría incluye un objetivo de control y uno o varios controles aplicables para lograrlo.

Las cláusulas que define el estándar son las siguientes:

1) Política de seguridad (1 categoría, 2 controles).
   Brinda un lineamiento de implementación del documento de la política de seguridad, así como la revisión del mismo.

2) Organización de la seguridad de la información (2 categorías, 11 controles).
   Fija un marco referencial para el manejo de la seguridad, tanto una organización interna, como hacia terceros.

3) Gestión de activos (2 categorías, 5 controles).
   Establece responsabilidades sobre los activos, así como su clasificación.

4) Seguridad de recursos humanos (3 categorías, 9 controles).
   Brinda una serie de controles a implantar antes, durante y en el cese o cambio de personal.

5) Seguridad física y ambiental (2 categorías, 13 controles).
   Indica medidas para establecer áreas seguras y la protección de equipo.

6) Gestión de comunicaciones y operaciones (10 categorías, 32 controles).
   Garantiza una apropiada operación de los medios de procesamiento de la información, como protección contra código malicioso, copias de seguridad, seguridad en redes, entre otros.

7) Control de acceso (7 categorías, 25 controles).
   Gestiona el control de acceso de usuarios, a la red, al sistema operativo, aplicaciones y equipo fuera de sitio.

8) Adquisición, desarrollo y mantenimiento de sistemas de información (6 categorías, 16 controles).
   Brinda los requisitos de seguridad necesarios para los sistemas de información.

9) Gestión de incidentes de seguridad de la información (2 categorías, 5 controles).
   Indica controles a implantar en el caso de eventos relacionados con la seguridad.

10) Gestión de la continuidad del negocio (1 categoría, 5 controles).
    Establece controles a aplicar en caso de una suspensión de las actividades comerciales, así como su protección. También brinda lineamientos para la implementación de planes de continuidad.

11) Conformidad (3 categorías de seguridad, 10 controles).
    Para el cumplimiento de requerimientos legales, de políticas y normas. También establece ciertas consideraciones para realizar auditorías a los sistemas de información.

CAPÍTULO 4

POLÍTICAS DE SEGURIDAD Y BUENAS PRÁCTICAS

Las ventajas que ofrece el plantear objetivos en la organización garantiza que la información manejada dentro y fuera del sistema central de la organización, cuente con los elementos necesarios para asegurar su protección contra alteración, divulgación o negación de acceso no autorizados, permitiendo la continuidad de las operaciones en las áreas de negocio principalmente o en áreas donde se maneja información secreta, confidencial o privada.

4.1 POLÍTICAS DE SEGURIDAD

El principal objetivo informático de la organización es dar protección y seguridad a su información, para ello es necesario establecer las normas, políticas y estándares de seguridad para los sistemas distribuidos que procesan, almacenan y transmiten información, a fin de minimizar los riesgos en su integridad, confidencialidad y disponibilidad.

Según María Jaquelina López y Cintia Quezada en su libro Fundamentos de Seguridad Informática. "La política de seguridad es un 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 informática dentro de la misma."[10]

La política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas. En sí es un conjunto de leyes, reglas y prácticas que permiten salvaguardar los activos de una organización y brindar seguridad dentro de ésta. Las políticas sirven para cumplir los objetivos de seguridad dentro de una organización.

Debe fielmente representar una política del mundo real y además debe interactuar con la política de recursos. En ella se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas. Así mismo, debe ser expresada en un lenguaje en el que todas las personas involucradas (quiénes crean la política, quiénes la van a aplicar y quiénes la van a cumplir) puedan entender.

A través de las leyes, reglas y prácticas que reflejen las metas y situaciones de la organización, ellas también reflejan los principios que se aplican en general.

Los principios fundamentales de una política son:

1. Responsabilidad individual: las personas son responsables de sus actos. El principio implica que la gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.
2. Autorización: son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.
3. Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

[10]María Jaquelina López y Cintia Quezada. Fundamentos de seguridad informática. UNAM. Facultad de Ingeniería, 2006. Página 129

4. Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad y función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.

5. Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.

6. Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

7. Reducción de riesgo: esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

La política de seguridad involucra papeles que se repiten en muchas situaciones y también en aplicaciones específicas. Para documentos realizados en papel se aplican los siguientes roles genéricos:

a) Originador (autor): es la persona que publica un documento, frecuentemente el autor o el director es el responsable de éste.

b) Autorizador: es la persona que tiene el control sobre el documento. Indica quién puede autorizar o denegar el acceso al mismo para editar, copiar, leer, etcétera. El autorizador puede o no ser el autor.

c) Custodio: es la persona que físicamente guarda el documento y lleva a cabo los propósitos del autorizador sobre la manera de accederlo.

d) Usuario: es la persona que lee y modifica el documento.

Si se trata de una transacción comercial, se aplican otros roles o funciones:

a) Creador: es la persona que diseña la transacción y escribe las reglas sobre los pasos por seguir.

b) Cliente: es la persona que en su nombre se lleva a cabo la transacción.

c) Ejecutor: es la persona que efectivamente realiza la transacción en nombre del cliente, paga un cheque, abre una cuenta, etcétera.

d) Supervisor: es la persona que verifica que las acciones, resultados y controles se hayan llevado a cabo conforme a lo establecido por el creador.

De las tres propiedades de seguridad más importantes (confidencialidad, integridad y disponibilidad), las dos primeras reflejan claramente las propiedades en el mundo real.

A continuación se mencionarán brevemente las políticas para éstas propiedades.

1) Políticas para la confidencialidad

Algunos documentos importantes son guardados en secreto para cualquiera, excepto para el propio creador. Los documentos son agrupados o clasificados de acuerdo con el tipo de confidencialidad que se necesite. La política puede ser indicada como una relación entre la clasificación del documento y la posición o cargo de la persona. Por ejemplo, políticas de confidencialidad con niveles de clasificación: súper secreto, secreto, confidencial o no clasificado.

2) Políticas y controles para la integridad

La administración en el control de la política está dirigida principalmente a la integridad más que a la confidencialidad porque para la mayoría de las aplicaciones empleadas como -sistemas financieros, comerciales, militares- es más importante mantener la integridad de los datos ya que cada vez se necesitan automatizar más actividades -sistemas de comunicación- que requieren de dispositivos y aplicaciones más complejos, de tal manera que es necesario mantener la integridad de éstos y la integridad de los datos que procesan.

A continuación se mencionan algunas de las políticas de integridad más comunes e importantes:

a) Política de acciones autorizadas. Establece que la gente puede realizar las acciones para las que está autorizada, esta política aplica para importantes medios. Por ejemplo, en una caja registradora.

b) Política de control supervisor. Ciertas acciones deben ser aprobadas por un supervisor.

c) Política de rotación de obligaciones. Una tarea no debe ser realizada siempre por la(s) misma(s) persona(s).

d) Política de control de “n” personas. Requiere que la gente coopere para llevar a cabo una acción.

e) Política de secuencia de operaciones. Requiere que los pasos de alguna tarea deban llevarse a cabo en un orden específico. Frecuentemente esta política es combinada con la separación de obligaciones y “n” personas de control, así que una persona o grupo diferente realiza cada paso de la secuencia.

f) Política de cambio restringido. Requiere que la información sea cambiada siempre en la forma prescrita y estructurada, es decir, que desde que se diseña la política hay que considerar que se pueden presentar cambios y éstos pueden realizarse respetando y siguiendo determinados procedimientos que se hayan elaborado previamente.

g) Política de atribución de cambios. Tiene como objetivo verificar la validez de la información.

3) Políticas de seguridad de la computación.

La política de seguridad debe ser específica. Las políticas seleccionadas deben ser hechas sobre la situación actual de los sistemas conectados en red. Una política de seguridad debe estar especificada en un documento especial para tal propósito, redactada en un lenguaje natural, claro y sin ambigüedades posibles. El documento deberá especificar qué propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas.

La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas de información y que proporciona las bases para definir y delimitar responsabilidades para las diversas acciones técnicas y organizativas que se requerirán.

La política se refleja en una serie de normas, reglamentos y protocolos por seguir, donde se definen las distintas medidas que se van a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su funcionamiento.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, con lo que los procesos más importantes recibirán más protección.

El compromiso de los directivos con la seguridad de los sistemas de información debe tomar la forma de una política de seguridad de los sistemas de información formalmente acordada y documentada. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos ya que muchas amenazas (incendio o inundación) son comunes a otras actividades de la organización.

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

a) Toda política de seguridad debe cubrir todos los aspectos relacionados con el sistema.

b) Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.

c) Debe tomar en cuenta los distintos componentes del sistema (hardware, software, entorno físico y usuarios), así como la interacción entre los mismos.

d) Debe tomar en cuenta el entorno del sistema, el tipo de compañía.

e) La política de seguridad debe adecuarse a las necesidades y recursos, el valor que se le da a los recursos y a la información, el uso que se hace del sistema en todos los departamentos.

f) 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.

g) Debe adoptar el modelo “Todo lo que no esté específicamente prohibido está permitido” o bien, el que dice “Todo está prohibido excepto lo que esté específicamente permitido”

Recordar que al momento de establecer una política de seguridad es vital responder a las tres preguntas básicas:

a) ¿Qué se necesita proteger?

b) ¿De qué se necesita proteger?

c) ¿Cómo se va a proteger?

Y para lograrlo se necesita lo siguiente:

a) Determinar los recursos por proteger y su valor.

b) Analizar las vulnerabilidades y amenazas del sistema, probabilidad de ocurrencia y su costo.

c) Definir las medidas por establecer para proteger el sistema, se debe definir una estrategia en caso de falla.

d) Verificar el cumplimiento de la política, revisarla y mejorarla cada vez que se detecte un problema.

Las políticas de seguridad, son el marco de referencia de la seguridad, en ellas se define lo que está permitido y lo que está prohibido, permiten definir procedimientos necesarios, responsabilidades y tareas.

Existen formas para redactar las políticas de seguridad. Cuando se redacta un conjunto de políticas se decide una filosofía (aunque las 2 primeras son las más utilizadas):

a) Prohibitivas

Todo está prohibido a excepción de los que está permitido. Por ejemplo: evitar fumar en el salón. “Todo está prohibido excepto lo que esté específicamente permitido”

b) Permisivas

Todo está permitido a excepción de lo que está prohibido. Por ejemplo: se prohíbe fumar en el salón. “Todo lo que no esté específicamente prohibido está permitido”

c) Paranoica.

Nada está permitido.

d) Promiscua.

Todo está permitido.

Es recomendable que las políticas se elaboren considerando los siguientes puntos:

a) Recopilar material de apoyo

Para elaborar el conjunto de políticas de seguridad informática, debe efectuarse previamente un análisis de riesgo que indique las necesidades de seguridad actuales de la organización.

Se deben conocer los antecedentes de fallas en la seguridad, fraudes, demandas judiciales. Además de tener copia de todas las otras políticas de organización referentes a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los temas que serán cubiertos dentro del conjunto de políticas de seguridad. La lista debe incluir políticas que se piensan aplicar de inmediato, así como aquellas que se piensan aplicar en el futuro.

c) Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se redactan las políticas.

Las políticas van dirigidas a audiencias distintas, por lo que se aconseja redactar documentos diferentes de acuerdo con el tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporcione más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la presidencia y junta directiva para su aprobación. Este comité debe tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar las políticas, analizar el costo/beneficio y sus implicaciones.

Las preguntas que se debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables?, ¿Son estas políticas claras e inequívocas?

Las siguientes personas son responsables, en distintos grados, de la seguridad en la organización:

1) El Comité de Seguridad Informática está compuesto por los representantes de los distintos departamentos de la organización, así como por el gerente de informática, el gerente de telecomunicaciones (cuando exista), y el abogado o representante legal de la compañía. Este comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el comité efectuará la evaluación y revisión de la situación en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos que afecten la seguridad.

2) La gerencia de informática es responsable de establecer y vigilar el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la junta directiva y la gerencia de telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e

implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

3) El jefe de seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

4) El administrador de sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra. También es responsable de informar al jefe de seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un jefe de seguridad, el administrador de sistemas realizará sus funciones.

5) Los usuarios son responsables de cumplir con todas las políticas de la organización referentes a la seguridad informática y en particular:

   - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
   - No divulgar información confidencial de la organización a personas no autorizadas.
   - No permitir y no facilitar el uso de los sistemas informáticos de la organización a personas no autorizadas.
   - No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la organización.
   - Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
   - Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo y otras asociaciones parecidas.
   - Reportar inmediatamente a su jefe inmediato a un funcionario de seguridad informática cualquier evento que pueda comprometer la seguridad de la organización y sus recursos informáticos, por ejemplo, contagio de virus, intrusos, modificación o pérdida de datos.
   - Deben leer y firmar de aceptación sobre las políticas de seguridad antes de otorgárseles acceso a los recursos.

La metodología para desarrollar, implementar, realizar el mantenimiento de las políticas de seguridad. (Figura 4.1) se muestra a continuación:

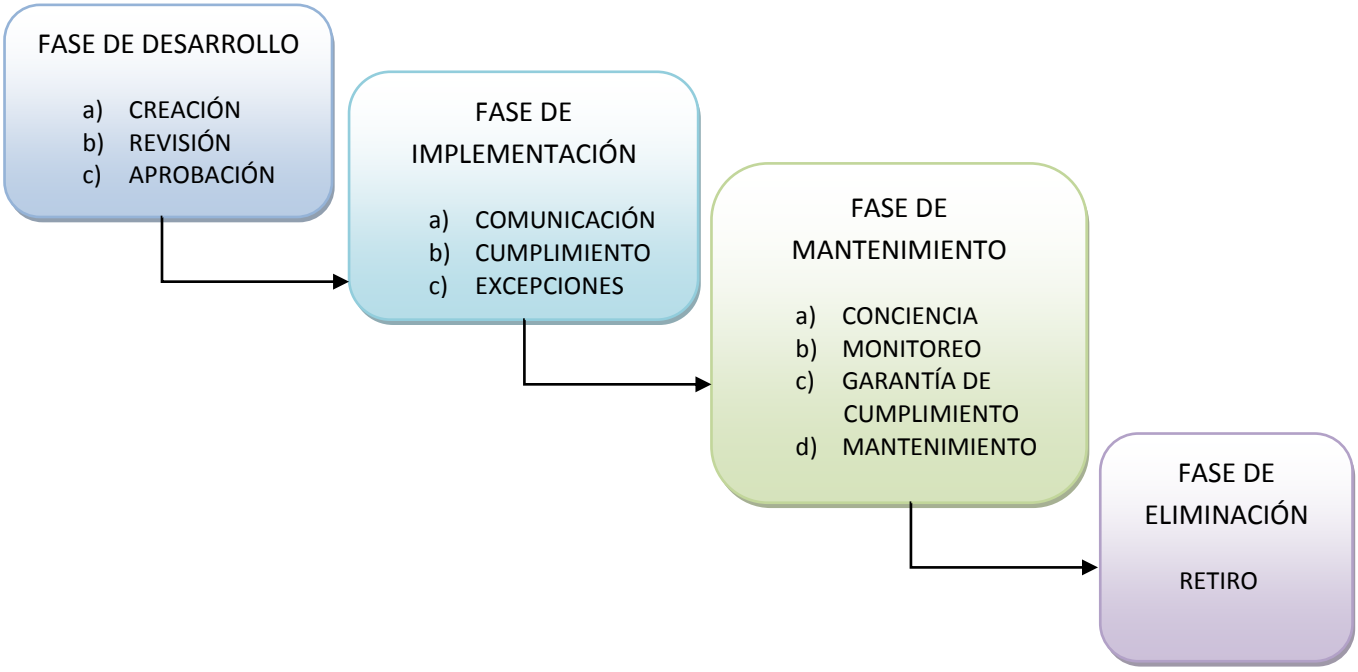

Figura 4.1 Metodología para políticas de seguridad

Hay once etapas que deben realizarse a través de la vida de una política. Estas etapas se clasifican en cuatro fases.

1. Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.

   a) Creación: planificación, investigación, documentación y coordinación de la política.

      El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política, es decir, la creación. La creación de una política implica identificar por qué se necesita la política, determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, qué autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción).

   b) Revisión: evaluación independiente de la política.

      Una vez que la documentación de la política ha sido creada, ésta debe ser remitida a un grupo independiente para su evaluación antes de su aprobación final.

c) Aprobación: obtener la aprobación de la política por parte de las directivas.

El objetivo de esta etapa es obtener el apoyo de la organización, a través de la aprobación de la persona con autoridad.

2. Fase de implementación: en esta fase la política es comunicada y atacada (o no cumplida por alguna excepción).

a) Comunicación: difundir la política.

La política debe ser inicialmente difundida a los miembros de la organización. Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

b) Cumplimiento: implementar la política.

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Dentro de esta etapa se elaboran informes de la implementación de la política.

c) Excepciones: gestionar las situaciones donde la implementación no es posible.

Debido a que hay problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando se amerite, es probable que se requieran excepciones a la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción.

3. Fase de mantenimiento: los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

a) Concienciación: garantiza la conciencia continuada de la política.

Es la fase de mantenimiento, comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento. La etapa de concienciación incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento.

b) Monitoreo: seguimiento y reporte del cumplimiento de la política.

Esta etapa es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Es monitoreada para informar el cumplimiento o no de la política, reportando las deficiencias encontradas.

c) Garantía de cumplimiento: afrontar las contravenciones de la política.

Incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Una vez que la contravención sea identificada, la acción correctiva debe ser determinada y

aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

d) Mantenimiento: asegurar que la política esté actualizada.

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios que puede afectar la política; recomendado y coordinando modificaciones, documentándolos en la política y registrando las actividades de cambio. Esta etapa garantiza la disponibilidad continuada, al igual que el mantenimiento de la integridad de la política a través de un control. Cuando se requieran cambios en la política, las etapas realizadas antes deben revisarse, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

4. Fase de eliminación: la política se retira cuando no se requiera más.

a) Retiro: prescindir de la política cuando no se necesite más.

Después que la política ha cumplido con su finalidad y no es necesaria, entonces debe ser retirada. Esta etapa corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Con esto se evitan confusiones posteriores, es necesario archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera)

Algunas prácticas recomendadas para escribir una política son las siguientes:

1. La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular)
2. Nombre y cargo de quién autoriza o aprueba la política.
3. Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política.
4. Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento.
5. Indicadores para saber si se cumple o no la política.
6. Referencias a otras políticas y regulaciones con las que se tiene relación.
7. Enunciar el proceso para solicitar excepciones.
8. Describir los pasos para solicitar cambios o actualizaciones a la política.
9. Explicar qué acciones se seguirán en caso de contravenir la política.
10. Fecha a partir de la cual tiene vigencia la política.

11. Fecha de cuándo se revisará la conveniencia y la obsolescencia de la política.
12. Incluir la dirección de correo electrónico, la página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias.

Otras prácticas que se recomiendan seguir son:

1. Uso de lenguaje sencillo.
2. Escribir la política como si fuese a utilizarse siempre.
3. Debe escribirse de tal forma que pueda leerlo cualquier miembro de la organización.
4. Se debe evitar describir técnicas o métodos particulares que definan una sola forma de hacer las cosas.
5. Cuando se requiera, hacer referencia explícita y clara a otras dependencias de la organización.
6. Utilizar una guía para la presentación de documentos escritos.

Es importante considerar que al redactar las políticas de seguridad se debe redactar en tiempo presente.

También se debe considerar que las políticas de seguridad son fundamentales en la administración de la seguridad de una organización. Deberán ser evaluadas periódicamente para que concuerden con la misión de la seguridad.

En el momento de que ocurra un incidente de seguridad, las políticas indicarán quiénes tienen la debida autoridad para tomar acciones que mitiguen el impacto de éste y evitar que se repita.

Permiten identificar y eventualmente sancionar a los responsables. Para una correcta redacción de las políticas, se deberá conjuntar un equipo, incluyendo a la alta administración, conformado por personal que tenga la experiencia y capacidad necesaria para la tarea.

Se deberá indicar el alcance de las políticas al inicio del proceso de redacción, que sea consistente con la misión de seguridad de la organización.

Asimismo, deberán contener ciertos rubros como la definición de la seguridad, objetivos, importancia, un enunciado de la intención de la dirección de la organización, un marco referencial (incluyendo una breve descripción de la gestión de riesgos), consecuencias de la violación de alguna política y referencias.

Se debe también tomar en cuenta que las políticas que no sean del todo aceptadas por los usuarios, serán difíciles de implantar, a menos que se indiquen sanciones que logren el cumplimiento de éstas aunque cuenten con una aceptación entusiasta.

Al final, no deberá contarse con políticas que afecten la productividad o la misión de la organización. Debe indicarse en cada política los responsables, las acciones y los periodos de validez, es decir quién, qué y cuándo.

La adopción de un mecanismo de seguridad deberá ser justificada por una o más políticas. Todo control deberá contar con procedimientos de operación, administración y contingencia. Se deberá evitar que las políticas sean inconsistentes entre sí y evitar contradicciones.

Deben considerarse ciertos puntos de importancia organizacional como: protección y clasificación de los recursos, separación de funciones, monitoreo, mínimo privilegio, redundancia, continuidad, actualización, cultura, ética, administración y mejores prácticas.

4.2 BUENAS PRÁCTICAS

Para obtener un mejor desempeño en la organización son necesarios diferentes controles y análisis. En la actualidad, es necesario conocer y practicar los aspectos de seguridad en las organizaciones, además de llevar a cabo las medidas de seguridad necesarias.

A estas medidas, controles y análisis se le adicionan recomendaciones, las cuales son indispensables para obtener el mejor nivel de seguridad deseado. A este tipo de recomendaciones también se les conoce como prácticas, las cuales surgen de la experiencia o de quienes han elaborado estas recomendaciones.

Estas prácticas son utilizadas en todo tipo de organizaciones con la finalidad de mejorar el desempeño del personal que labora, no son obligatorias pero son necesarias.

Es decir, las buenas prácticas son recomendaciones o consejos que se le dan al personal durante su trabajo o al momento de su capacitación, para que éste desarrolle de manera eficiente el trabajo, resuelva o evite problemas relacionados con las actividades a realizar. Lo indispensable es que estas prácticas o recomendaciones se lleven a cabo para un mejor desempeño. Aunque no es obligatorio conocerlas en su totalidad, es necesario que el personal las considere y realice.

Las buenas prácticas recogen experiencias en seguridad, las cuales son aplicadas a instituciones como son: educativas, gubernamentales, comerciales, etcétera. Regularmente, este tipo de buenas prácticas se apoyan en algunas políticas de seguridad de la misma organización o se basan en la experiencia del personal en esa área, de esta forma se desarrollan las prácticas.

Es decir, se ve a las buenas prácticas como un método cuya efectividad ha sido probada y validada por la experiencia de aplicación en una actividad relacionada con la seguridad. Otra manera de entender el concepto de las buenas prácticas; son lineamientos, recomendaciones o prácticas de tipo no obligatorio que resultan ser efectivas para la realización de actividades, trabajos o tareas que se requieren desarrollar dentro de la organización. Las buenas prácticas se deben desarrollar en un documento para que sean leídas y consideradas por todo el personal.

Una de las principales ventajas de las buenas prácticas es poder incorporar a los usuarios de manera rápida a las actividades y no tener que capacitar de una manera formal. Sin embargo, para evitar problemas y conflictos internos éstas deben estar basadas en las políticas internas de la organización. Estas buenas prácticas deben haber sido aprobadas por la misma organización como un documento anexo o una extensión para usos prácticos de las políticas de seguridad que se estén llevando a cabo dentro de la organización.

Algunas características de las buenas prácticas son:

a) Permiten incorporar al personal de manera rápida a las actividades.

b) Deben estar basadas y reguladas en las políticas de seguridad.

c) No son de carácter obligatorio.

d) Son recomendaciones para ayudar al usuario a realizar mejor sus actividades.

e) Deben ser reguladas por las políticas de seguridad.

f) Pueden estar basadas en la experiencia personal.

g) No delega responsabilidades.

h) Ayuda al personal a la realización de actividades sencillas y básicas.

En el ámbito de la seguridad informática, las buenas prácticas están integradas por un conjunto de políticas y normas específicas cuyo objetivo es la protección de los activos en una organización. Al ser implementadas ayudan a mitigar los principales problemas de seguridad a los que se encuentra expuesta, logrando como resultado mejorar su desempeño.

A continuación se mencionan algunas características generales de las buenas prácticas:

a) No son disposiciones legales y no deben interpretarse como tales.

b) Reflejan medidas prudentes y efectivas que las instituciones han implementado o están en proceso de implementar.

c) Para proteger efectivamente información y garantizar la disponibilidad, confidencialidad e integridad.

d) Deben verse en el contexto de las necesidades de la organización.

e) Algunas buenas prácticas parecen simples y obvias pero son esenciales.

Sólo cuatro buenas prácticas se ven como elementales:

1. Desarrollo de política de seguridad.
2. Clasificación de la información.
3. Cifrado de información altamente confidencial.
4. Autenticación fuerte para control de acceso a sistemas críticos.

Las buenas prácticas se deben llevar a cabo en la organización, si en el centro de cómputo se cuenta con TI, de igual manera se deben contemplar buenas prácticas para ellas.

Las TI se entienden, como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. Las TI se encuentran generalmente asociadas con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

Las tecnologías de la información y la comunicación, también conocidas como TIC's, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro o procesar información para poder calcular resultados y elaborar informes.

Las TIC's agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones. Es decir, son el conjunto de tecnologías desarrolladas para gestionar, procesar, almacenar, recuperar y transmitir información.

Algunas características de las TIC's son:

- Interactividad.
- Canales de comunicación inmediata.
- Innovación. Dan acceso a nuevas formas de comunicación.
- Interrelación de imagen y sonido.
- Mayor influencia y beneficios, cuando es bien aplicada, a los sectores productivos, económicos, educativos, etcétera, de una sociedad.
- Interconexión.
- Diversidad de tecnologías.

Algunos ejemplos de los usos de las TIC's son: (Figura 4.2)

- Internet de banda ancha.
- Teléfonos móviles de última generación.
- Televisión de alta definición.
- Códigos de barras para gestionar los productos en un supermercado.
- Bandas magnéticas para operar con seguridad con las tarjetas de crédito.
- Cámaras digitales.
- Reproductores de MP3.

Figura 4.2 Ejemplos de las Tecnologías de la Información y la Comunicación

Las TIC's son herramientas teórico-conceptuales; soportes y canales que procesan, almacenan sintetizan, recuperan y presentan información de la forma más variada. Los soportes han evolucionado en el transcurso del tiempo (telégrafo óptico, teléfono fijo, celulares, televisión) ahora, en esta era, se puede hablar de la computadora y de la Internet. El uso de las TIC's representa una variación notable en la sociedad y, a la larga, un cambio en la educación, en las relaciones interpersonales y en la forma de difundir y generar conocimientos.

Las tecnologías de la información y la comunicación están presentes y han transformado la vida. Esta revolución ha sido propiciada por la aparición de la tecnología digital. La tecnología digital, unida a la aparición de computadoras cada vez más potentes, ha permitido a la humanidad progresar muy rápidamente en la ciencia y la técnica desplegando el arma más poderosa: la información y el conocimiento.

Algunas ventajas de las TIC's son:

- Brindar grandes beneficios y adelantos en salud y educación.
- Permitir el aprendizaje interactivo y la educación a distancia.
- Impartir nuevos conocimientos para la empleabilidad que requieren muchas competencias (integración, trabajo en equipo, motivación, disciplina, etcétera.)
- Ofrecer nuevas formas de trabajo.

- Difundir información de interés en todos los rubros: culturales, administrativos, económicos, sociales, etcétera, a un amplio sector.
- Permitir la agilización y simplificación de procesos de índole diversa a nivel global.
- Optimizar recursos.
- Agilizar la comunicación en audio y video.
- Controlar el acceso a la información, así como al área de trabajo.
- Se tiene mayor comunicación entre diferentes entidades en tiempo real.
- Mayor eficiencia en las producciones de un país.
- Incremento de la creatividad.
- Se motivan las habilidades y actitudes sociales.
- Mayores opciones de transmitir la información.
- En el ámbito educativo: crear material didáctico para facilitar el aprendizaje.
- Acceso a la comunicación desde cualquier lugar.
- Rápida difusión de las investigaciones.
- Colaboración entre personas de distintos países para un bien común. Por ejemplo: la salud.
- Han permitido que muchas personas tengan acceso a estudiar o capacitarse a distancia, vía Internet. Estudiar una carrera universitaria a través de Internet.
- Acceder a cursos para la formación permanente.
- Facilitar el acceso a la educación y a la cultura.
- Fomentar el aprendizaje cooperativo y colaborativo.
- Mejorar el aprovechamiento de los recursos.
- Motivación e interés en desarrollar nuevas tecnologías para facilitar la integración de más personas en el uso de las tecnologías.
- Desarrollan habilidades en la búsqueda de la información.
- Permiten el aprendizaje interactivo.
- Debido a las amplias herramientas, se simplifica el trabajo de una persona, sin necesidad de estar en un lugar fijo.
- Estimula la investigación.

Desventajas de las TIC'S:

- Riesgo de fraude.
- Pérdida de los puestos de trabajo debido a la automatización de las tareas.
- Falta de seguridad.
- Riesgo de comprometer la información de carácter personal.
- Pérdida de la privacidad en las diferentes redes de comunicación.
- Pérdida del interés social. No resulta interesante involucrarse en los problemas del exterior, aunque se afecte indirectamente.
- Algunas personas tienden a ser egocentristas con otras debido a que tienen más apego a las tecnologías.
- Pérdida de honestidad y humildad.
- Desequilibrio social.
- Deterioro de las relaciones humanas.
- Pérdida de valores sociales.
- Dependencia de la tecnología.

- Pérdida de tiempo.
- Hay un desequilibrio en el desarrollo de la personalidad.
- Ventilación de información personal.
- Son costosas, debido al avance de las tecnologías, éstas tienden a quedarse descontinuadas, lo que obliga a actualizar y aprender nuevas herramientas.
- Aislamiento familiar.
- Uso inadecuado de las tecnologías: pornografía, extorsión, etcétera.
- Despidos laborales justificados por falta de preparación o interés de las personas por ajustarse a las nuevas formas de trabajo en donde se integran las TIC's.
- Falta de capacitación continua.
- Inversión de recursos, tiempo y dinero.
- Demandan tiempo y esfuerzo.
- Pérdida de objetivos, tiempo y dinero. Con el uso del Internet se tiende a la distracción y, por ende, a la disminución de la productividad real de las personas en las empresas u organizaciones.
- El interés al estudio pueda que sea sustituido por la curiosidad y exploración en la web en actividades no académicas tales como juegos, música, videos, redes sociales, etcétera.
- Falta de análisis y comprensión de la información.
- Puede fomentarse la transmisión de información errónea dentro de la red.

En todas las áreas de la gestión empresarial, las TIC's han transformado la manera de trabajar, haciendo las cargas de trabajo menos pesadas, optimizando los recursos y elevando la productividad. Gracias a esto, se produce más y con una mejor calidad, invirtiendo mucho menos tiempo.

La tecnología es dual por naturaleza ya que el impacto de ésta dependerá del uso que le dé el usuario: se puede ayudar a una comunidad rural a aprender por medio de la televisión, como también se puede explotar una bomba por medio de un teléfono celular. Por tal motivo, se habla de la implicación de las tecnologías dentro de la construcción social.

Las TIC's han llegado a ser uno de los pilares básicos de la sociedad y hoy es necesario proporcionar una educación que tome en cuenta esta realidad. Las posibilidades educativas de las TIC's deben ser consideradas en dos aspectos: su conocimiento y su uso.

El primer aspecto es consecuencia directa de la cultura de la sociedad actual. Es preciso entender cómo se genera, cómo se almacena, cómo se transforma, cómo se transmite y cómo se accede a la información en sus múltiples manifestaciones (textos, imágenes, sonidos) si no se quiere estar al margen de las corrientes culturales.

El segundo aspecto es más técnico. Se deben usar las TIC's para aprender y para enseñar. Es decir, el aprendizaje de cualquier materia o habilidad se puede facilitar mediante las TIC's y, en particular, mediante Internet, aplicando las técnicas adecuadas. Este segundo aspecto tiene que ver muy ajustadamente con la informática educativa.

No es fácil practicar una enseñanza de las TIC's que resuelva todos los problemas que se presentan, pero hay que tratar de desarrollar sistemas de enseñanza que relacionen los distintos aspectos de

la Informática y de la transmisión de información, siendo al mismo tiempo lo más constructivos que sea posible desde el punto de vista metodológico.

Requiere un gran esfuerzo de cada profesor implicado y un trabajo importante de planificación y coordinación del equipo de profesores. Aunque es un trabajo muy motivador, surgen tareas, tales como la preparación de materiales adecuados para el alumno. Se trata de crear una enseñanza de forma que teoría, abstracción, diseño y experimentación estén integrados.

Las discusiones que se han venido manteniendo por los distintos grupos de trabajo interesados en el tema se enfocaron en dos posiciones. Una consiste en incluir asignaturas de Informática en los planes de estudio y la segunda en modificar las materias convencionales teniendo en cuenta la presencia de las TIC's.

Actualmente se piensa que ambas posturas han de ser tomadas en consideración y no se contraponen. De cualquier forma, es fundamental para introducir la informática en la escuela, la sensibilización e iniciación de los profesores a la informática, sobre todo cuando se quiere introducir por áreas (como contenido curricular y como medio didáctico).

Por lo tanto, los programas dirigidos a la formación de los profesores en el uso educativo de las nuevas tecnologías de la información y comunicación deben proponerse como objetivos:

- Contribuir a la actualización del Sistema Educativo que una sociedad fuertemente influida por las nuevas tecnologías demanda.
- Facilitar a los profesores la adquisición de bases teóricas y destrezas operativas que les permitan integrar, en su práctica docente, los medios didácticos en general y los basados en nuevas tecnologías en particular.
- Adquirir una visión global sobre la integración de las nuevas tecnologías en el currículum, analizando las modificaciones que sufren sus diferentes elementos: contenidos, metodología, evaluación, etcétera.
- Capacitar a los profesores para reflexionar sobre su propia práctica, evaluando el papel y la contribución de estos medios al proceso de enseñanza-aprendizaje.

Finalmente, hay que buscar las oportunidades de ayuda o de mejora en la educación explorando las posibilidades educativas de las TIC's en todos los entornos y circunstancias que la realidad presenta.

La incorporación responsable de las TIC's es un elemento clave en la gestión, considerando que la adopción de estas tecnologías ya no es una opción, sino una necesidad creciente para insertarse en la actual sociedad de la información y responder a los requerimientos del mercado globalizado.

Las TIC's son herramientas eficaces para la gestión de la información, la flexibilización del tiempo y el flujo de la comunicación. Su aporte en la academia es creciente ya que, entre otras:

- Permiten un aprendizaje y trabajo colaborativo.

- Reducen costos y tiempos de trabajo.

- Controlar recursos y asuntos administrativos.
- Facilitan la comunicación interna y externa.

Para entender qué significan y cuáles son las utilidades de las tecnologías, como también conocer cómo se usan, es preciso generar una difusión de buenas prácticas relativas a estas herramientas.

Las buenas prácticas son una forma de organizar y desarrollar una tarea, actividad o proceso para lograr los resultados deseados. Considerando que es necesario llevar a cabo un manual de buenas prácticas, para tener con esto, una guía que incorpore un conjunto de recomendaciones. El manual recogerá y difundirá experiencias innovadoras para que sirvan de modelo.

En la redacción de las buenas prácticas se debe procurar:

a) Innovación. Implementar acciones complementarias respecto a lo ya establecido.
b) Soluciones a problemas. Implementando acciones pertinentes en función de las causas y factores involucrados.
c) Orientación al logro de los objetivos de interés para conseguir los resultados perseguidos dentro de la misión de las TIC's.
d) Elementos dirigidos a la incorporación de tecnologías. Se busca promover el uso de las TIC's.
e) Integración. Para proporcionar trabajo colaborativo, intercambio de información y la comunicación.
f) Eficiencia. Para optimizar el uso de los recursos que se utilizan en su implementación.

Para su elaboración y difusión es necesaria la recopilación de estas experiencias positivas con el fin de retroalimentar y favorecer el aprendizaje del centro de cómputo.

Para ello se debe llevar a cabo un control desde su elaboración hasta su evaluación. Tomando esto en cuenta, a continuación se explica el ciclo de las buenas prácticas.

1. Evaluar las experiencias y aprender las lecciones.
2. Captar las buenas prácticas y organizar la documentación.
3. Compartir y difundir buenas prácticas.
4. Adoptar, adaptar y aplicar las buenas prácticas.

Cabe señalar la importancia de retroalimentar el ciclo de las buenas prácticas (Figura 4.3) para tener mejores resultados.

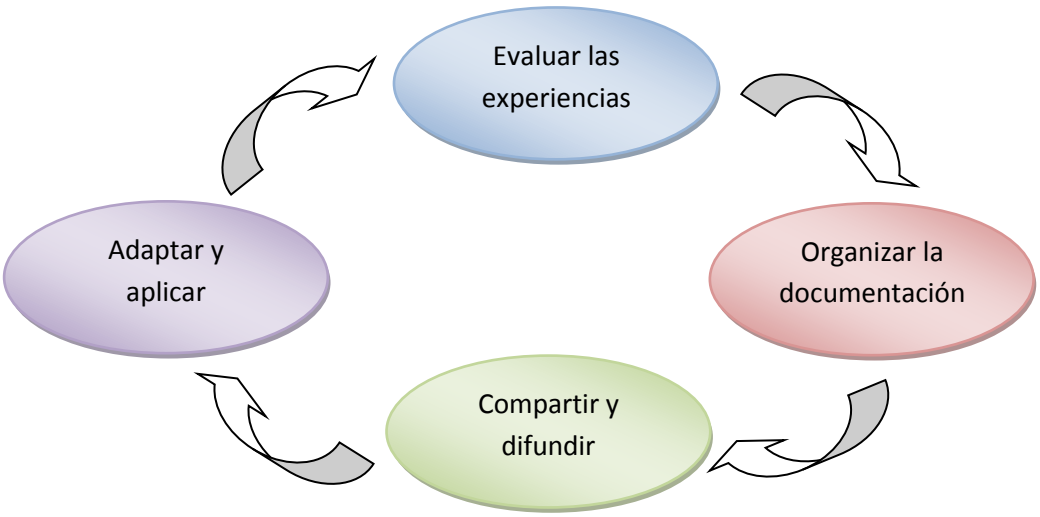

Figura 4.3 Ciclo de las buenas prácticas

Las buenas prácticas abarcan los sistemas de seguridad que la organización requiera, por ejemplo.

En la seguridad física, se incluyen normas y procedimientos para asegurar, edificios, computadoras, medios de comunicación.

El objetivo es minimizar el riesgo de robo o destrucción del recurso. Es la primera línea de defensa para los sistemas de información.

Se protege el sistema contra la obtención de acceso a los recursos de forma indebida, daño accidental del hardware como resultado imprevisto de otras actividades.

La implementación de las buenas prácticas se lleva a cabo por medio de reglas administrativas, procedimientos y mecanismos físicos.

Por ejemplo, una regla administrativa es quién o quiénes están autorizados a entrar a qué áreas sensibles. En los procedimientos y mecanismos físicos se tienen las cerraduras, tarjetas magnéticas de identificación, aislamiento físico de hardware sensible, funciones de trabajo, etcétera.

También se involucran aspectos relacionados con la construcción del edificio, asignación de lugares, procedimientos de emergencia, reglamentos de relacionados con el uso de las fuentes de energía y relaciones con empleados y agencias.

Algunas buenas prácticas aplicables a la seguridad física son:

- En áreas críticas o sensibles se debe contar con equipos de seguridad física para evitar daños, tanto a la información como al hardware.
- Instruir al personal sobre su uso y su funcionamiento de los equipos. Por ejemplo: en alarmas, extintores de fuego, detectores de humo, salidas de emergencia, etcétera.

Esto, con el objetivo de evitar daños físicos al personal, a la información y a los equipos de hardware.

CAPÍTULO 5

GUÍA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN UN CENTRO DE CÓMPUTO

Actualmente, la adopción de las tecnologías de la información es una necesidad creciente para involucrarse en la actual sociedad de la información, para así responder a los requerimientos diarios.

Algunos aportes importantes que se tiene por adoptar las tecnologías de la información son:

- Permitir un aprendizaje y trabajo colaborativo
- Reducir costos y tiempos de trabajo
- Controlar recursos y asuntos administrativos
- Facilitar la comunicación interna y externa

Para comenzar a elaborar las buenas prácticas se debe organizar y desarrollar una actividad o un proceso que persigue el logro de los resultados deseados, fundamentalmente desde la perspectiva del aprendizaje de las personas.

5.1 PROPUESTA DE BUENAS PRÁCTICAS EN UN CENTRO DE CÓMPUTO

El objetivo del desarrollo de buenas prácticas es recoger y difundir experiencias innovadoras que sirvan de modelo para los integrantes del centro de cómputo. Con esto se busca generar la colaboración entre los involucrados a través del intercambio de experiencias para optimizar los recursos existentes.

Para facilitar el uso de las buenas prácticas se sugiere llevar a cabo un manual de buenas prácticas, la cual será una guía que incorporará un conjunto de recomendaciones para el fin propuesto. A continuación se muestra un esquema de los pasos a seguir para proponer buenas prácticas. (Figura 5.1)

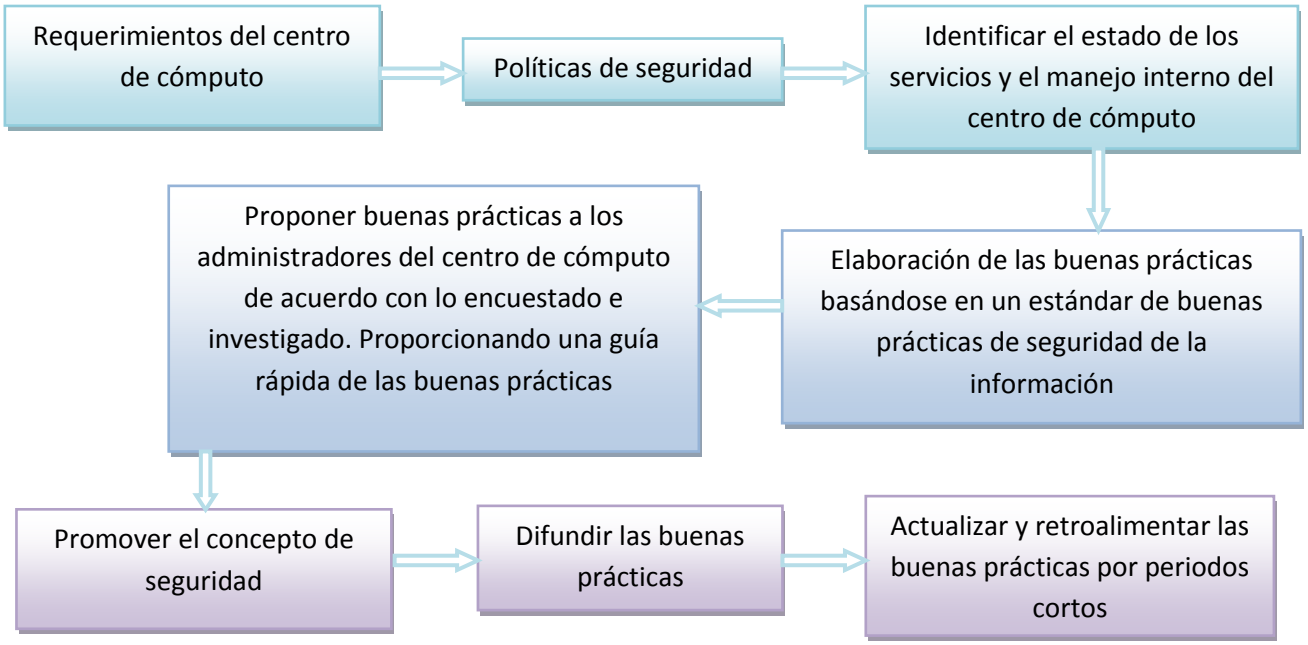

Figura 5.1 Aspectos para proponer nuevas prácticas

Al proponer las buenas prácticas se deben considerar los siguientes aspectos:

1. REQUERIMIENTOS NECESARIOS DEL CENTRO DE CÓMPUTO PARA DAR SERVICIO

Se van a establecer las bases para determinar los requerimientos con base en las funciones del centro de cómputo, es decir dependiendo del área al que va dirigido, sea docente, administrativa, de consulta, etcétera. De manera general, se debe definir la forma en que se prestarán sus servicios en las diferentes áreas. Teniendo en cuenta que la computadora es una herramienta de solución para problemas de cálculo, investigación, procesos, enseñanza, entre otros.

Los requerimientos, respecto a la seguridad física en el centro de cómputo son:

a) Ubicación física del centro de cómputo

   Es necesario conocer la importancia de los equipos principales como servidores, esto para tener medidas de seguridad acordes con las características del equipo a proteger. Se debe seleccionar la ubicación buscando la parte más conservadora, la cual debe estar lejos del área de usuario, de equipos eléctricos con el propósito de resguardar el equipo para que el servicio no se interrumpa.

   Se recomienda que las instalaciones del centro de cómputo sean construidas en edificios o áreas separadas, considerando la planeación de la distribución física del equipo de cómputo, áreas de iluminación, aire acondicionado; colocar ventiladores, vidrios polarizados o persianas ya que la luz solar afecta directamente a los equipos.

   También considerar los riesgos respecto a desastres naturales como inundaciones, fallas eléctricas, polvo, incendios, entre otros. Evitar vibraciones de maquinaria pesada ya que afecta los equipos.

b) Instalaciones físicas del centro de cómputo

   Es importante seleccionar el lugar correcto para el buen funcionamiento del centro de cómputo, considerando cuestiones del ambiente externo. Considerando si se está expuesto a peligros naturales como el frío, el calor, las lluvias, sismos, inundaciones y hundimiento de piso, para prevenir este tipo de peligros naturales es necesario llevar a cabo una planificación en la distribución de servidores y equipos de usuario considerando los aspectos anteriores, además de elaborar un plan de recuperación.

   Considerar que el local tenga los servicios básicos que se requieren, que estén disponibles y en buen funcionamiento, por ejemplo energía eléctrica, ventilación, líneas telefónicas, cobertura inalámbrica y drenaje.

   Para brindar un servicio eficiente es necesario considerar la zona en la que está ubicado el centro de cómputo, que no esté expuesto a riesgos, la zona debe ser concurrida, que alrededor no se ubiquen fábricas de cartón, gas, pinturas, ningún tipo de fábrica flamable o propensa a incendios.

Es necesaria la instalación de piso falso, considerando la resistencia que debe tener para soportar el peso del equipo de cómputo, del personal y usuarios. Es importante señalar que el cableado debe quedar debajo del piso falso y colocar techo falso donde tenga conexiones internas de aire acondicionado.

c) Control de acceso físico

Colocar puertas grandes y salidas de emergencia. Considerando las dimensiones entre puertas y ventanas para tener una buena iluminación en el centro de cómputo.

d) Aire acondicionado

Es necesaria la instalación de aire acondicionado para que no se sobrecalienten los equipos y brinden un mejor funcionamiento. Se deben instalar equipos de aire acondicionado, de acuerdo al tamaño del centro de cómputo. Además de instalar alarmas para la humedad, temperatura flujos de aire.

e) Instalación eléctrica

Es de gran importancia la instalación eléctrica en el centro de cómputo ya que todo el funcionamiento depende de ella, por lo que una falla puede llegar a provocar grandes daños al equipo y detener los servicios del mismo. Se requieren colocar reguladores de voltaje independientes en servidores y equipos de cómputo.

f) Riesgo de inundación

Considerar el peligro a inundaciones, es recomendable que el centro de cómputo esté situado en los pisos más altos y no en la planta baja.

g) Protección, detección y extinción de incendios

Se requiere instalar extinguidores y detectores de incendios.

h) Mantenimiento

Se debe dar mantenimiento a las instalaciones para que no se tengan daños considerables y el centro de cómputo no interrumpa el servicio.

En el centro de cómputo se identifican tres principales Departamentos:

a) Soporte técnico a usuarios. El soporte, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar, instalar y mantener el sistema operativo.

b) Gestión y administración del centro de cómputo. La administración debe mantener y desarrollar la infraestructura de red. El administrador de red debe estar atento y mantener actualizados sus conocimientos para poder modernizar la infraestructura de la red. Además de operar el sistema de computación y mantener el sistema disponible para los usuarios.

c) Departamento de seguridad en cómputo. La seguridad en cómputo brinda una mejor efectividad y eficiencia de los servicios del centro de cómputo. Se ocupa de monitorear los procesos y las aplicaciones realizadas por los usuarios, realizar revisiones periódicas en la red e instalaciones. Realizar bitácoras de incidentes y dar soluciones oportunas y efectivas para que el servicio no se interrumpa. Y retroalimentar de acuerdo con lo revisado con la administración y monitoreo del sistema, cambios o actualizaciones del centro de cómputo.

Para tener una visión organizada de los componentes que requiere el centro de cómputo, se pueden dividir sus elementos en dos categorías: hardware y software.

a) Hardware

Se recomienda que se verifique que el equipo adquirido cumpla con los requerimientos solicitados, además de realizar una evaluación económica respecto al costo/beneficio y la efectividad para realizar el trabajo. Por ejemplo, costos al adquirir servidores, equipos de cómputo, impresora, escáner y reguladores de energía, entre otros.

b) Software

Se recomienda, realizar un análisis del software que se requiera, es decir paquetería de acuerdo con la dirección del negocio (hacia quién va a estar dirigido). Por ejemplo, sistemas operativos (Windows, Linux, etc.), office, open office, photoshop, corel drawn, autocad, matlab, entre otros.

2. POLÍTICAS DE SEGURIDAD

Con base en las políticas ya creadas por el centro de cómputo, éstas se toman en cuenta para ofrecer mayor seguridad a los servicios brindados y regular la manera de dirigir, proteger y distribuir recursos en el centro de cómputo.

Teniendo en cuenta que las políticas deben ser apoyadas por los directivos, deben ser únicas, y bien estructuradas, su redacción debe ser clara, breve y de manera positiva. Además de darlas a conocer por escrito y deben ser entendidas por los usuarios. Es importante señalar que deben actualizarlas por periodos o al integrar nuevas tecnologías

De no contar con políticas de seguridad, se recomienda revisar el apartado de políticas de seguridad en el Capítulo 4 de este trabajo para saber cómo realizarlas.

3. IDENTIFICAR EL ESTADO DE LOS SERVICIOS Y EL MANEJO INTERNO DEL CENTRO DE CÓMPUTO

Para identificar el estado de los servicios se recomienda llevar a cabo un breve cuestionario que proporcione información de los servicios y el manejo interno del centro de cómputo. A continuación se plantea un ejemplo base de un cuestionario para conocer los tipos de servicios que puede ofrecer un centro de cómputo, así como el manejo interno que tendrá.

1. ¿A qué tipo de personas está dirigido el centro de cómputo?
2. ¿Cuál es su uso? Académico/Consulta/Otro.

3. ¿Qué servicios brindará?
4. ¿Cuáles son los requerimientos de red?
5. ¿Cuáles son los requerimientos de software?
6. ¿Cuáles son los requerimientos del sistema operativo?
7. ¿Cuáles son los requerimientos de navegadores de red?
8. ¿Cuáles son los requerimientos de impresoras?
9. ¿Cuáles son los requerimientos de escáner?
10. ¿Se requieren copiadoras?
11. ¿Se requiere que los usuarios descarguen programas y documentos?
12. ¿Se cuenta con un Departamento de seguridad y monitoreo de la red?
13. El personal involucrado, ¿Tiene conocimiento de la seguridad informática?
14. ¿La información se mantiene íntegra, disponible y confidencial para los interesados del centro de cómputo?, ¿La información es restringida?
15. ¿Se cuenta con un plan de recuperación, en caso de que ocurra un fraude, sabotaje, los cuáles pueden provocar la destrucción parcial o total de la información?
16. ¿Se cuenta con herramientas de prevención o detección, en caso de que se introduzca un virus, troyano, etcétera?
17. En caso de contar con antivirus, antimalware, antispyware, etc., ¿Está actualizado, configurado, se realiza un escaneo del sistema, se revisa periódicamente?
18. ¿Se instala software pirata? Se recomienda que no sea así ya que puede afectar la funcionalidad, eficiencia y disponibilidad, viéndose afectada la disponibilidad de los equipos de cómputo y la red.
19. ¿La computadora se utiliza adecuadamente?, ¿Únicamente es para uso laboral?
20. ¿Se cuenta con elementos administrativos?
21. Respecto al personal del centro de cómputo, ¿Se cuenta con una definición clara de las políticas de seguridad?
22. ¿Los empleados y usuarios del centro de cómputo identifican las políticas de seguridad?
23. ¿Los empleados y usuarios del centro de cómputo identifican las buenas prácticas?
24. ¿Se cuenta con un plan de organización y prevención de desastres?
25. ¿Se cuenta con sistemas de seguridad en equipos, incluyendo elementos de redes?
26. ¿Se cuenta con aplicaciones para los sistemas de seguridad, datos y archivos?
27. ¿Se cuenta con un auditor de sistemas (ajeno a la organización)?
28. ¿Se realiza periódicamente la planeación de programas y pruebas?
29. ¿Se eleva el nivel de riesgo que puede tener la información? Esto para poder hacer un adecuado estudio costo/beneficio por sistema.
30. ¿Se clasifica la instalación en términos de riesgo?
31. ¿Se identifican las aplicaciones de alto riesgo?
32. ¿Se cuantifica el impacto en caso de suspensión del servicio en aquellas aplicaciones de alto riesgo?
33. ¿Se formulan medidas de seguridad?

34. ¿Hay un buen rendimiento? Implicando eficiencia y eficacia (teniendo una buena administración.
35. ¿Hay una buena planeación, organización, dirección y control? ¿Se realiza periódicamente?

Respondiendo a estas preguntas se tendrá un panorama más amplio de los servicios que se requieren brindar, saber si se pueden mejorar las medidas de seguridad y la mejor manera de organizar al personal involucrado, como soporte, administradores y el departamento de seguridad. Con el principal objetivo de ofrecer un mejor servicio a los usuarios y proporcionar la confianza que requieren para utilizar el centro de cómputo.

4. ELABORACIÓN DE LAS BUENAS PRÁCTICAS BASÁNDOSE EN UN ESTÁNDAR DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN

La importancia de realizar correctamente las buenas prácticas es establecer controles de seguridad para la información y los activos. Brindando así, protección en procedimientos y técnicas dentro del centro de cómputo.

Es indispensable basarse en estándares para proteger la información y garantizar la implementación de las estrategias que propician la tríada de la seguridad.

Esta propuesta de buenas prácticas para implementar la seguridad en un centro de cómputo, es elaborada con base en COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas-Control Objectives for Information and related Technology).[11]

Se seleccionó COBIT porque en los objetivos de control se brinda calidad, gestión y correcta administración en los servicios prestados, abordando también temas de seguridad asociados a los servicios a través de un marco de trabajo de dominios y procesos.

Para la elaboración de las buenas prácticas se considerará COBIT orientado a procesos. Con base al esquema de trabajo de COBIT se pretende asegurar el servicio y brindar mejoras en las medidas de seguridad proponiendo buenas prácticas para la implementación de seguridad en un centro de cómputo. Para proporcionar un mayor enfoque en el desempeño del centro de cómputo.
A continuación se muestra el esquema de trabajo de COBIT, detallando cada proceso de sus cuatro dominios. (Figura 5.2)

[11] Véase Anexo A

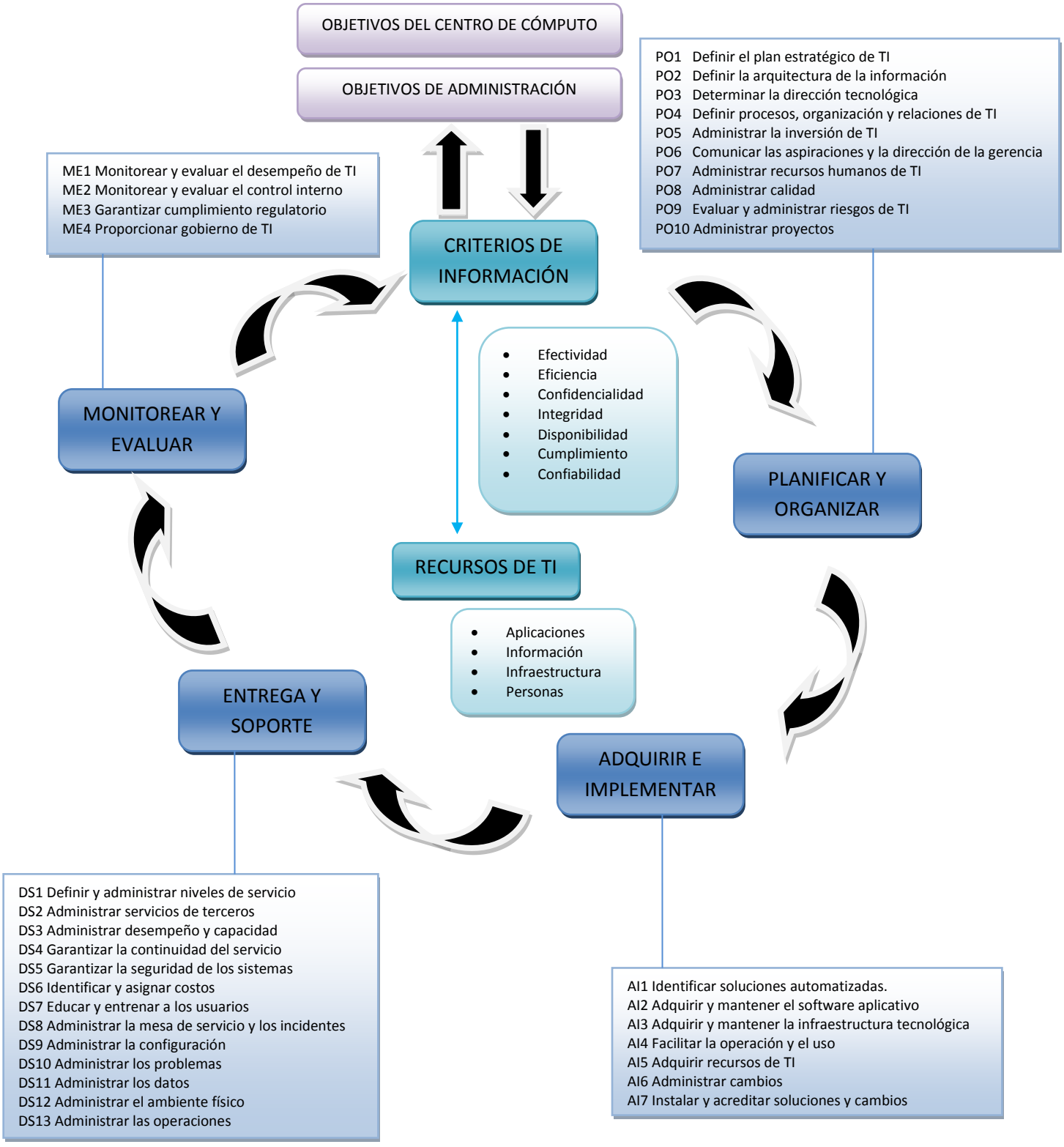

Figura 5.2 Marco de trabajo de COBIT

5. PROPONER BUENAS PRÁCTICAS PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN UN CENTRO DE CÓMPUTO

Para lograr un uso exitoso de las TIC's e incorporarlas en el trabajo diario, se debe prestar atención a las prácticas que se desarrollan al interior del centro de cómputo. Es importante señalar que se deben respetar las sugerencias o acciones y toma de decisiones, para así reforzar la gestión del centro de cómputo con base en las TIC's.

A continuación se presenta la propuesta de buenas prácticas con base en COBIT, basándose en sus cuatro dominios.

1) PLANEAR Y ORGANIZAR

a. PO1 Definir el plan estratégico de TI

Los encargados del centro de cómputo deben alinear la planeación estratégica de TI con las necesidades iniciales y futuras. El plan estratégico se utiliza para establecer las metas a futuro.

Pasos para definir un plan estratégico.

- Realizar una evaluación de las tecnologías que incluya el valor económico de las mismas.
- Enseñar a los encargados las capacidades tecnológicas actuales y las oportunidades que ofrecen las TIC's.
- Definir los objetivos estratégicos o las metas, así como los costos y riesgos relacionados.
- Llevar a cabo un análisis describiendo los proyectos y servicios, así como los beneficios logrados.
- Administrar regularmente los cambios en las TIC's, realizando un documento que contenga: la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.
- Evaluar el desempeño de los planes existentes y de los sistemas de información.
- Al finalizar la evaluación se debe corroborar que se esté contribuyendo con los objetivos, su funcionalidad, estabilidad, costos y fortalezas.

Buenas prácticas

- ✓ Se debe realizar un plan estratégico siguiendo los pasos antes mencionados, el cual defina las oportunidades de crecimiento y las limitaciones que tendrá el centro de cómputo. Esto para satisfacer los requerimientos y estrategias del lugar, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos.
- ✓ Se deben especificar objetivos concisos, planes de acción, tareas comprendidas y aceptadas por los encargados del centro de cómputo.
- ✓ Implementar un esquema de prioridades, identificando las áreas estratégicas para considerar los requerimientos del centro de cómputo.
- ✓ Los responsables del centro de cómputo deben identificar la capacidad y evaluar el desempeño de los involucrados en el centro de cómputo.

- ✓ Se recomienda que los empleados del centro de cómputo conozcan el plan de desarrollo, con esto se pretende que se sientan motivados para realizar su trabajo con lo mejor de sus habilidades.

b. PO2 Definir la arquitectura de la información

Se debe agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente para integrar las aplicaciones dentro de los procesos del centro de cómputo.

Buenas prácticas

- ✓ Crear y actualizar regularmente un modelo de información, para realizar el estudio, análisis, organización, disposición y estructuración de la información.

- ✓ Se deben definir sistemas apropiados para optimizar el uso de esta información.

- ✓ Establecer un modelo de datos que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos para asegurar que se proporciona información confiable y segura.

- ✓ Clasificar la información, es decir, asignar el tipo de información a los interesados correctos, sean encargados, administradores, técnicos, etcétera.

c. PO3 Determinar la dirección tecnológica

Al determinar la dirección tecnológica, primero se analizan las tecnologías existentes, se crea un plan de infraestructura tecnológica, se monitorean las tendencias y regulaciones futuras.

Buenas prácticas

- ✓ Determinar la dirección tecnológica para dar soporte al centro de cómputo.

- ✓ Establecer y administrar las expectativas claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.

- ✓ Actualizar la información, respecto a la arquitectura de sistemas, dirección tecnológica, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios.

d. PO4 Definir procesos, organización y relaciones de TI

Al definir los procesos con relación a las TIC's, se establecerá una estructura organizacional del centro de cómputo, definir las tareas o roles, así como las responsabilidades de los involucrados.

Por ejemplo:

Los encargados son los responsables de que se cumpla con las políticas y buenas prácticas. Los administradores, responsables de brindar una mejor seguridad en los sistemas de información.

Los técnicos, responsables de apoyar a los usuarios para que no se cometan errores, que de ser graves pueden ser un riesgo alto para el centro de cómputo.

Buenas prácticas

- ✓ Delimitar o definir los requerimientos del centro de cómputo, tomando en cuenta los requerimientos del personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión.

- ✓ Establecer estructuras organizacionales transparentes, flexibles y responsables en la integración de roles y responsabilidades hacia los procesos del centro de cómputo.

- ✓ Se debe redactar un escrito, definiendo los roles y responsabilidades para el personal involucrado.

- ✓ Establecer y mantener relaciones de comunicación y coordinación.

e. PO5 Administrar la inversión de TI

Para administrar las inversiones en las TIC's, se asignarán los presupuestos, se medirá y evaluará el costo/beneficio hacia las inversiones.

Buenas prácticas

- ✓ Establecer y mantener un marco de trabajo para administrar los programas de inversión en las TIC's que abarquen costos, beneficios y prioridades dentro del presupuesto.

- ✓ Establecer y administrar presupuestos de las TIC's, de acuerdo con la estrategia y las decisiones de inversión para que sean efectivas y eficientes para estados actuales y futuros del centro de cómputo.

f. PO6 Comunicar las aspiraciones y la dirección de la gerencia

Buenas prácticas

- ✓ Se debe asegurar comunicar los objetivos del centro de cómputo hacia las TIC's.

- ✓ Proporcionar procedimientos y documentación de forma precisa y entendible sobre los servicios de las TIC´s actuales y futuros.

- ✓ Definir, implementar, difundir y administrar las políticas de las TIC's de acuerdo con las nuevas tecnologías.

g. PO7 Administrar recursos humanos de TI

Al administrar los recursos humanos, se pretende adquirir gente competente y motivada para crear y entregar servicios de TI.

Buenas prácticas

- ✓ Los responsables de recursos humanos, deben contratar personal capacitado, los directivos deben proporcionarles constantemente cursos, diplomados o incentivos para que se sientan motivados y se actualicen con las nuevas tecnologías. Proporcionándoles planes a futuro, asignándoles roles respecto a sus habilidades. Esto para que cubran las expectativas y los requerimientos para el centro de cómputo.

- ✓ Revisar y evaluar el desempeño del personal. Con esto se pretende mitigar el riesgo sobre la dependencia de recursos arcaicos.

- ✓ Realizar procedimientos de investigación o proyectos.

h. PO8 Administrar calidad

La administración de calidad se lleva con base en la definición de estándares y prácticas de calidad definidas.

Buenas prácticas

- ✓ Se recomienda realizar un plan de calidad que promueva la mejora continua.

- ✓ Investigar e identificar estándares y prácticas de calidad de acuerdo con las necesidades internas del centro de cómputo.

- ✓ Medir, monitorear y revisar el plan de calidad.

i. PO9 Evaluar y administrar riesgos de TI

Al evaluar y administrar los riesgos se pretende brindar seguridad al centro de cómputo, al analizar y comunicar los riesgos de TI y su impacto sobre las metas del centro de cómputo. La administración de los riesgos internos y externos debe ser consistente.

Buenas prácticas

- ✓ Crear y dar mantenimiento a un marco de trabajo de administración de riesgos.

- ✓ Realizar evaluaciones de riesgo

- ✓ Desarrollar y mantener un proceso de respuesta a los riesgos

- ✓ Mantener y monitorear un plan de acción de riesgos

j. PO10 Administrar proyectos

Este proceso, satisface la entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados.

Buenas prácticas

- ✓ Se deben planear proyectos. Definiendo y documentando el alcance, recursos y responsabilidades del proyecto.
- ✓ Establecer un enfoque de administración de proyectos. Administrando los riesgos y establecer controles sobre cambios del proyecto.
- ✓ Medir el desempeño, reportar y monitorear el proyecto.
- ✓ Finalizar el proyecto, asegurándose de proporcionar los resultados esperados.

De manera general para el dominio planear y organizar se proponen las siguientes buenas prácticas:

- ✓ Antes de dar servicio, se recomienda formular las medidas de seguridad necesarias para el centro de cómputo.
- ✓ Se recomienda evaluar el desempeño inicial del centro de cómputo, calificando la capacidad del personal involucrado con los requerimientos del centro de cómputo.
- ✓ Se recomienda proponer un esquema de prioridades para los objetivos del centro de cómputo. Para que los administradores y encargados alineen la planeación de las TIC's con las necesidades actuales y futuras del centro de cómputo.
- ✓ Se recomienda elaborar un diseño base de lo que se va a necesitar para cubrir sus requerimientos para ofrecer servicios, como la elección del equipo de cómputo, las instalaciones, la orientación del centro de cómputo (a qué tipo de usuarios está dirigido), el tipo de conexión que se necesitará, equipo de trabajo (administradores, desarrolladores, técnicos), etcétera.
- ✓ Se recomienda propiciar una buena relación entre encargados y administradores, se les deben mostrar las ventajas del uso de las TIC's las oportunidades actuales y futuras para establecer las prioridades del centro de cómputo.
- ✓ Se recomienda generar dos tipos de comunicaciones: una motivacional (por qué y para qué usar las TIC's) y otra informativa (qué recursos existen, cómo pueden usarse).
- ✓ Para estimular la comunicación y coordinación entre las diferentes áreas involucradas, la recomendación es fomentar la unión entre los involucrados para desarrollar una armonía productiva, para así promover el trabajo colaborativo, con un estilo multidireccional, abierto y cooperativo, con características como, creatividad, flexibilidad y cooperación. Donde cada miembro es productor, usuario y comunicador de conocimiento. Es necesario promover procesos de integración.
- ✓ Se debe elaborar un plan estratégico, en cooperación con los interesados, donde se describirán y discutirán las iniciativas de las TIC's con los requerimientos del centro de cómputo.

- ✓ Se recomienda formular el reglamento de ingreso al centro de cómputo ya que si los usuarios entran con dispositivos como teléfonos, iphone, tabletas, etcétera. Debe indicarse que son responsabilidad de cada usuario.

- ✓ Es recomendable planear periódicamente la elaboración de proyectos, investigaciones, asesorías, transferencias, visitas de expertos, congresos.

- ✓ Se recomienda promover el área de investigación con proyectos y publicaciones. Al innovar, se requiere la transferencia de conocimientos internos y externos. Esto permite el desarrollo de nuevas metodologías, estrategias, recursos y herramientas que constituyen un factor clave para un aprendizaje mediado por tecnologías.

- ✓ Se recomienda contar con personal calificado en esta materia, que actúe no sólo de soporte técnico, sino que también como desarrollador, tanto en la actualización y creación de nuevos sistemas adecuados a las necesidades del centro de cómputo. En este contexto este personal debe también asesorar a los usuarios, ya sean estudiantes, docentes, investigadores, autoridades y administrativos.

- ✓ Dejar claro que es un centro de cómputo y por lo tanto queda estrictamente prohibido, fumar, comer y beber en el centro de cómputo, se recomienda colocar señalamientos en lugares visibles que recuerden dicha prohibición.

- ✓ Se recomienda colocar extintores y un botiquín de primeros auxilios, en caso de que ocurra algún accidente. Así como colocar señalamientos visibles dentro del centro de cómputo.

- ✓ Se recomienda asignar lugares apropiados para los discos externos, papelería y herramientas de trabajo.

- ✓ Se recomienda que se verifique el aire acondicionado ya que constantemente los filtros del aire se tapan y para evitar esto se debe limpiar periódicamente, también se debe contar con una fuente no interrumpible de energía eléctrica.

- ✓ Se recomienda trabajar conjuntamente. Todo el personal de un área, departamento o asignado a una tarea debe conocer las tareas (siendo el responsable una persona) esto para darle un seguimiento, por si algún encargado llega a faltar.

- ✓ Se recomienda que se le especifiquen al usuario las aplicaciones, programas y archivos que deben usarse.

- ✓ Se recomienda la planeación de programas y pruebas.

- ✓ Se recomienda que los encargados y administradores clasifiquen los datos e información que sean de valor para el centro de cómputo.

- ✓ Se recomienda tener un control del número de computadoras (nodos) que se encuentren conectadas a la red. Esto debe estar en un documento para acceder rápidamente.

- ✓ Se recomienda que el administrador del centro de cómputo se encargue de ejercer el liderazgo entre su personal, para la toma de decisiones, también es quien debe encargarse de la evaluación y la compra de hardware y software para el buen funcionamiento del centro de cómputo.

- ✓ Respecto a la ubicación física, se requiere tener un control de computadoras. Es conveniente realizar un croquis o un esquema del diseño del centro de cómputo, indicando la ubicación de los nodos (indispensables y de reserva), el servidor, las computadoras, impresoras y escáner.

- ✓ Se debe informar a los usuarios las recomendaciones del uso de dispositivos como impresoras, escáneres, fax. Por ejemplo, impresiones a color (imágenes, gráficas, etc.) o blanco/negro (solo texto). El tipo de hojas permitidas, grosor, tamaño, forma y color etcétera.

- ✓ Se recomienda que al momento de adquirir un equipo se deban tener en cuenta, los requerimientos que cumplirá. La compra de equipo debe ser evaluada económicamente y la efectividad del trabajo en el que se utilizará.

- ✓ Se recomienda comunicarle a los usuarios las reglas de acceso al centro de cómputo, ya sea que se les pida identificación o que se les proporcione una credencial especial expedida por los encargados del centro de cómputo, corroborando que al final del uso de equipo todo esté en orden.

- ✓ Considerar que no todos los usuarios son expertos en cómputo, por lo que el mal uso de sus equipos compromete la seguridad de la información o servicios del centro de cómputo. Así que se recomienda que el usuario se interese y cumpla con las políticas de seguridad, reglamentos de contraseñas, de control de acceso, de uso adecuado, de respaldos, de correo electrónico, del uso de direcciones IP, de sitios web, de contratación, de auditoría, de plan de contingencias y las sanciones en caso de no cumplir con los reglamentos.

- ✓ Se recomienda capacitar periódicamente a los integrantes del centro de cómputo con la finalidad de que se familiaricen con las nuevas tecnologías y tengan un mayor desempeño en sus labores para que disminuyan los incidentes y fallas en los equipos. En la capacitación se debe contar con ejemplos y casos prácticos que faciliten la participación en los procesos de resolución de problemas de manera crítica y reflexiva, fomentando así la interacción social (colaboración). Esto para que se presente el menor grado de incidentes.

- ✓ Cuando se realicen cursos de capacitación es recomendable que los contenidos sean presentados en multimedia (combinación de sonido, texto e imágenes) y acompañados como material de apoyo con documentos impresos y CD, debe contarse con la formación

de grupos de trabajo y foros de discusión, además de guías de aprendizaje elaboradas por expertos en tecnologías.

- ✓ Se recomienda procurar dar siempre respuesta a las dudas que se tengan, así como animar y fomentar el desarrollo del trabajo cooperativo para estimular el intercambio de conocimientos.
- ✓ Dependerá del centro de cómputo si les proporcionará a los usuarios usar espacio en disco duro para sus documentos. De preferencia, se recomienda que solo hagan uso de equipo de cómputo para revisiones, modificaciones, consultas de correos, documentos. Si quieren realizar modificaciones y guardar sus documentos, es preferible que los almacenen en sus propias unidades extraíbles o discos duros externos. En este caso se debe informar a los usuarios que el centro de cómputo no se hace responsable de documentos guardados en el equipo.

2) ADQUIRIR E IMPLEMENTAR

a. AI1 Identificar soluciones automatizadas.

Traduce los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas, enfocándose en la identificación de soluciones factibles y rentables.

Buenas prácticas

- ✓ Se recomienda definir y dar mantenimiento a los requerimientos técnicos y funcionales del centro de cómputo.
- ✓ Realizar estudios de factibilidad para recopilar datos relevantes sobre el desarrollo del centro de cómputo y con base en ello tomar la mejor decisión para su implementación. Por ejemplo: analizar y definir la arquitectura del equipo, la solución de problemas, contratos con proveedores.
- ✓ Se deben conocer y comprender las características del centro de cómputo así como los problemas que generaría, antes de iniciar la evaluación técnica que permita definir la arquitectura que se va a emplear. Es decir, primero indicar un panorama esperado, con lo que se cuenta (lo que se tiene) y los posibles resultados. Para así ubicar posibles errores que salgan sobre la marcha.
- ✓ Identificar, documentar y analizar los riesgos asociados con los requerimientos del centro de cómputo. Sin perder de vista cumplir con los requerimientos.
- ✓ Se debe considerar en el centro de cómputo invertir en equipos, por ejemplo, por futuras expansiones.

b. AI2 Adquirir y mantener el software aplicativo

Adquirir o construir las aplicaciones de acuerdo con los requerimientos del centro de cómputo, enfocándose en garantizar que exista un proceso de desarrollo oportuno y confiable.

Buenas prácticas

- ✓ Se recomienda documentar el diseño detallado.
- ✓ Administrar los requerimientos de aplicaciones. (Aplicaciones de editores de texto, de video, de diseño, sonido, de web, etcétera. De acuerdo con la orientación o hacia qué personas va a estar dirigido el centro de cómputo).
- ✓ Configurar e implementar el software de aplicaciones.
- ✓ Garantizar la funcionalidad del software realizando revisiones periódicas en su configuración y actualización de las aplicaciones, esto para asegurar la disponibilidad de las aplicaciones.

c. AI3 Adquirir y mantener la infraestructura tecnológica

Buenas prácticas

- ✓ Se deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica.
- ✓ Implementar medidas de control interno, seguridad y auditabilidad para la protección y disponibilidad del recurso de infraestructura

d. AI4 Facilitar la operación y el uso

Buenas prácticas

- ✓ Se recomienda desarrollar la documentación adecuada disponible para transferir el conocimiento. Es decir, generar y proporcionar manuales y materiales de entrenamiento necesarios para el uso exitoso de sistema.
- ✓ Comunicación y entrenamiento a usuarios, encargados, personal de apoyo y al personal de operación para transferir el conocimiento a usuarios finales.

e. AI5 Adquirir recursos de TI

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios.

Buenas prácticas

- ✓ Proteger y hacer cumplir los intereses del centro de cómputo al adquirir recursos de TI.
- ✓ Desarrollar un control de adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos.
- ✓ Formular un procedimiento para la administración de contratos con proveedores.

f. AI6 Administrar cambios

Todos los cambios deben administrarse formalmente y controladamente. Enfocándose en controlar la evaluación del impacto, autorización e implantación de todos los cambios a la infraestructura de TI.

Buenas prácticas

- ✓ Definir y comunicar los procedimientos de cambio, incluyendo cambios de emergencia.
- ✓ Evaluar y asignar la prioridad y autorización de cambios.
- ✓ Documentar el cambio al finalizar el análisis. Darle seguimiento y reportar el estatus del cambio.

g. AI7 Instalar y acreditar soluciones y cambios

Buenas prácticas

- ✓ Se debe establecer una metodología de prueba con procedimientos después de la implementación.
- ✓ Realizar y darle seguimiento a las pruebas.
- ✓ Evaluar los resultados de las pruebas.

De manera general para el dominio adquirir e implementar se proponen las siguientes buenas prácticas:

- ✓ Se recomienda instalar las actualizaciones de los sistemas operativos para que no contenga ningún error que produzca un agujero de seguridad. E instalar las actualizaciones de las aplicaciones de seguridad.
- ✓ Se recomienda que los navegadores estén actualizados, también los complementos que se utilicen. Recordarles a los usuarios no guardar sus contraseñas, ni formularios. También se deben eliminar del historial de exploración como: archivos temporales de Internet, cookies, datos de formularios, contraseñas, sitios web favoritos.
- ✓ Recomendarles a los usuarios utilizar el servicio únicamente para tareas del centro de cómputo, evitando curiosear. Debido a que el canal en el que viaja la información en Internet se considera promiscuo, ya que los mensajes pueden ser interceptados por un tercero, que escucha el canal y pueden ser sujetos de alteraciones maliciosas.
- ✓ Se recomienda buscar y encontrar controles técnicos, administrativos, legales, físicos para proteger a los activos con un costo razonable, conforme a las amenazas de mayor factor de riesgo. Los controles se clasifican en:

- Preventivos. Para evitar eventos que se supone pueden ocurrir. Por ejemplo, cifrado, control de acceso, análisis de riesgos, políticas.
- De detección. Para detectar eventos con la suficiente anticipación para tomar una medida. Por ejemplo, IDS, IPS, Anti código malicioso, etcétera.
- De recuperación. Para planear y y responder tan rápido como sea posible ante un evento y establecer un ambiente de operación segura.
- De garantía. Para asegurar que los controles implantados son efectivos. Por ejemplo, pentest, monitoreo periódico, revisión de seguridad de aplicaciones, apego a estándares, auditorías de seguridad, etcétera.

✓ Por parte del departamento de seguridad, es recomendable investigar las nuevas tecnologías para la seguridad en los equipos, así como las amenazas y vulnerabilidades recientes.

✓ Se recomienda la aplicación de los sistemas de seguridad para datos y archivos.

✓ Si el centro de cómputo comparte la red inalámbrica con los usuarios, establecer reglas de uso. Si los usuarios ingresan dispositivos como tablets, iphone's u otro tipo de dispositivo que puede utilizar la red inalámbrica, se recomienda contar con lineamientos para el uso de la red inalámbrica, así como formatos de responsiva, para que los usuarios se comprometan a hacer buen uso de ese servicio.

✓ Se recomienda desarrollar la creación de unidades de apoyo al centro de cómputo, las cuales fomenten el desarrollo de un aprendizaje y enseñanza a través de las tecnologías. Con el propósito de consolidar un valor colectivo desde el intercambio de experiencias y conocimientos.

✓ Elaborar y administrar regularmente un registro de las inversiones realizadas para lograr los objetivos por medio de la identificación, definición, evaluación, asignación de prioridades, selección del equipo de trabajo, administración, control de programas y selección del personal.

✓ Para garantizar la disponibilidad y rendimiento de los equipos. Se recomienda elaborar un calendario, citando las fechas en que se llevará a cabo el mantenimiento preventivo de hardware y software del centro de cómputo, así como la limpieza interna del centro de cómputo.

✓ Para restringir el acceso a todo el personal en la red. Se recomienda colocar en las sesiones permisos de administrador únicamente para la persona que se encuentra como responsable de los servicios (administrador de la red).

✓ Se recomienda que el administrador cuente con software de control de acceso en el equipo.

- ✓ Para que los usuarios utilicen el centro de cómputo. Se recomienda otorgar una cuenta de usuario sin privilegios, actualizar el sistema operativo, instalar software localmente o vía red, actualizar software crítico y antivirus.

- ✓ Se recomienda crear perfiles de usuarios con el objetivo de que los usuarios no gocen de acceso libre al sistema, con permisos bajo el perfil apropiado. Con el propósito de simplificar la administración de permisos, ofrecer mayor flexibilidad para especificar y vigilar la obediencia de las políticas de protección. Jerarquizando a los usuarios de menor a mayor.

  Por ejemplo, a continuación se especifican los objetos accesibles a perfiles (Tabla 5.1)

PERFIL	***ACCESO A***	***OPERACIONES***
Administrador	Toda la información	Lectura y escritura. Por ejemplo, para realizar un análisis del equipo y monitorear la red.
Apoyo técnico	Toda la información	Lectura
Usuario	Aplicaciones y servicios	Lectura

Tabla 5.1 Ejemplo de permisos

- ✓ Se recomienda la elaboración de bitácoras para mejorar la eficiencia, detectar cuellos de botella o errores en los programas. Otras bitácoras son diseñadas específicamente con la idea de seguridad informática en general y para la detección de intrusos en particular.

- ✓ Se recomienda realizar y administrar una bitácora con los movimientos diarios, sea de incidentes sucesos mínimos, cambios de equipo, reparaciones, etcétera. La bitácora debe ser de preferencia escrita y tener un respaldo digital, además debe contener fecha, nombre de la persona que escribe la nota. La revisión de bitácoras se debe hacer periódicamente y darle seguimiento a los acontecimientos, sean relevantes o no. Esto con el propósito de revisar las irregularidades y problemas de intrusión que pueda haber en el centro de cómputo.

- ✓ Para tener una seguridad en las contraseñas, se recomienda que los usuarios eviten pronunciar sus contraseñas en voz alta, que también eviten escribirlas en un papel que esté a la vista de las demás personas y que no usen la misma contraseña para todo. También no proporcionar a nadie sus contraseñas, de preferencia evitar colocar en las contraseñas fechas de nacimiento propias, de los hijos o esposo (a), domicilios, nombres de familiares, mascotas, personajes de ficción. En caso de equipos personales, evitar incluir el nombre de sesión en la contraseña, deben ser diferentes.

- ✓ Es recomendable que sus contraseñas sean robustas, que alterne letras, números y caracteres. Por ejemplo: combinar letra, números y caracteres para completar una oración que sólo usted conozca. Si por cualquier motivo debe proporcionarle a alguien su contraseña, se recomienda que sea usted quien la escriba, en caso que otra persona la escriba, deberá cambiarla enseguida.

- ✓ Se recomienda para la clave de la red colocar mecanismos de autenticación y métodos de cifrado.

- ✓ Debido al problema de pérdida de información, se recomienda realizar respaldos y actualizarlos cada 3 a 5 meses. Se recomienda no tener residuos de datos, es decir información que se encuentra almacenada en discos duros y unidades extraíbles, cd's que se desechan. Este tipo de información puede ser leída por otras personas que utilicen posteriormente ese medio, esto representa un riesgo al compartir archivos en disco o al tenerlos en desuso.

- ✓ Para tener un control de acceso adecuado dependiendo del área del centro de cómputo. Se recomienda: si es gubernamental, el control de acceso se permitirá por medio de firma digital o biometría, si es de uso pedagógico, utilizar credenciales de acceso, de acuerdo con los requerimientos y al presupuesto con el que se cuente. En el caso de credenciales, es necesario que el usuario proporcione nombre, teléfono, una fotografía y firma, por parte del centro de cómputo proporcionarle un número de identificador, la fecha y expedición, firma y sello de autorización.

- ✓ Para no tener interrupciones en los servicios, se recomienda tener cuidado que no exista virus o que no se tengan copias piratas de software que pueden afectar seriamente la imagen de la empresa, así como enfrentarse a demandas, multas, sanciones, etcétera.

- ✓ Al tener un crecimiento del centro de cómputo, con más equipo o mayor índice de usuarios, es recomendable contratar a más personal, ya que de no ser así peligra la seguridad del centro, porque no habrá quién cubra las diferentes áreas que lo contienen.

3) ENTREGAR Y DAR SOPORTE

a. DS1 Definir y administrar niveles de servicio

El definir y administrar niveles de servicio, se asegura la alineación de los servicios de las TIC's con la estrategia del centro de cómputo.

Buenas prácticas

- ✓ Se recomienda definir y administrar los servicios. Con la elaboración de un marco de trabajo.

- ✓ Formalizar acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega, la notificación del cumplimiento de los niveles de servicio (reportes y reuniones).

- ✓ Identificar y comunicar los requerimientos de servicios actualizados y nuevos.
- ✓ Monitorear y reportar el cumplimiento de los niveles de servicio.

b. DS2 Administrar servicios de terceros

Esto para brindar servicios satisfactorios ubicando los beneficios, riesgos y costos.

Buenas prácticas

- ✓ Revisar los contratos con los proveedores, identificando responsabilidades y servicios. Por medio de los acuerdos de contratación.
- ✓ Monitorear el desempeño del proveedor.

c. DS3 Administrar el desempeño y la capacidad

Esto con el propósito de optimizar el desempeño de los servicios, recursos y las capacidades de TIC's en respuesta a las necesidades del centro de cómputo.

Buenas prácticas

- ✓ Se debe establecer un proceso de planeación del desempeño, la capacidad y disponibilidad del sistema.
- ✓ Revisar la capacidad y el desempeño actual.
- ✓ Monitorear continuamente y realizar un reporte sobre el desempeño del sistema y la capacidad de los recursos de las TIC's.

d. DS4 Garantizar la continuidad del servicio

Asegurar el mínimo impacto en caso de una interrupción de servicios y ofrecer soluciones automatizadas, desarrollando, manteniendo y probando los planes de contingencia.

Buenas prácticas

- ✓ Desarrollar planes de contingencia de TI.
- ✓ Determinar los recursos críticos de TI.
- ✓ Realizar pruebas de contingencia de TI.
- ✓ Realizar mantenimiento (mejorando) del plan de contingencia de TI.
- ✓ Almacenar respaldos de los planes de contingencia y de los datos fuera de las instalaciones.

e. DS5 Garantizar la seguridad de los sistemas

Para mantener la integridad de la información y la protección de los activos.

Buenas prácticas

- ✓ Elaborar un proceso de administración de la seguridad de TIC's. Entendiendo y desglosando en un documento los requerimientos, vulnerabilidades y amenazas de seguridad.
- ✓ Se deben establecer y mantener los roles y responsabilidades de seguridad, políticas, estándares y procedimientos.
- ✓ Administrar cuentas del usuario (autorizaciones de los usuarios).
- ✓ Administrar claves criptográficas.
- ✓ Definir si hay incidentes de seguridad.
- ✓ Prevenir, detectar y corregir software malicioso.
- ✓ Monitorear, detectar, reportar y dar solución a las vulnerabilidades e incidentes de seguridad.
- ✓ Administrar la seguridad de la red. Realizando pruebas y monitoreando la red regularmente.

f. DS6 Identificar y asignar costos

Esto mejora la rentabilidad a través del uso bien informado de los servicios de las TIC's.

Buenas prácticas

- ✓ Definir los servicios.
- ✓ Llevar a cabo la contabilidad de las TIC's. Alineando la calidad y cantidad de los servicios brindados.

g. DS7 Educar y entrenar a los usuarios

Buenas prácticas

- ✓ Identificar las necesidades de entrenamiento y educación de los involucrados en el centro de cómputo.
- ✓ Organizar y establecer un programa de entrenamiento (periodos, fechas, horas, etc.)
- ✓ Evaluar el entrenamiento recibido.
- ✓ Monitorear y reportar la efectividad del entrenamiento. Realizando evaluaciones para el personal, como para usuarios finales.

h. DS8 Administrar la mesa de servicio y los incidentes

Al administrar los servicios e incidentes se responde de manera oportuna y efectiva las consultas y problemas de los usuarios en las TIC's.

Buenas prácticas

- ✓ Instalar y operar la mesa de servicios.
- ✓ Registrar las consultas de los usuarios.
- ✓ Establecer procedimientos para el monitoreo y resolución de incidentes.

i. DS9 Administrar la configuración

Buenas prácticas

- ✓ Realizar un reporte de todos los elementos de la configuración.
- ✓ Identificar y dar un mantenimiento a los elementos de configuración.
- ✓ Revisar la integridad de los datos de la configuración.

j. DS10 Administrar los problemas

Buenas prácticas

- ✓ Implementar procesos para identificar, clasificar y reportar los problemas (realizando un análisis de los problemas reportados).
- ✓ Rastrear y resolver los problemas progresivamente.
- ✓ Realizar un documento de los problemas con sus respectivas soluciones. Para consulta y almacenamiento del centro de cómputo.

k. DS11 Administrar los datos

Este proceso optimiza el uso de la información y garantiza la disponibilidad de la información cuando se requiera. Principalmente mantiene la integridad, disponibilidad y protección de los datos.

Buenas prácticas

- ✓ Verificar que todos los datos que sean procesados se reciban.
- ✓ Definir acuerdos de almacenamiento y conservación de datos.
- ✓ Definir e implementar los requerimientos de seguridad para la administración de datos. Para asegurar la transferencia o la eliminación de datos.
- ✓ Realizar un respaldo de los datos y restauración de los sistemas. (De preferencia fuera de las instalaciones)

- ✓ De ser requerido, establecer la manera segura de desechar los datos y el equipo.

l. DS12 Administrar el ambiente físico

El objetivo es proteger los activos de cómputo y la información, minimizando el riesgo de una interrupción del servicio. Con el propósito de proporcionar y mantener un ambiente físico adecuado para proteger los activos de TIC's contra acceso, daño o robo.

Buenas prácticas

- ✓ Definir e implementar medidas de seguridad física.
- ✓ Definir e implementar procedimientos para otorgar, limitar y revocar el acceso físico.
- ✓ Definir e implementar medidas de protección contra factores ambientales.
- ✓ Administrar las instalaciones físicas.

m. DS13 Administrar las operaciones

Este proceso incluye la definición de políticas y procedimientos de operación.

Buenas prácticas

- ✓ Administrar el procesamiento de información.
- ✓ Organizar la programación de tareas.
- ✓ Definir e implementar procedimientos para monitorear los servicios de TI.
- ✓ Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de las TIC's.
- ✓ Definir e implementar procedimientos de mantenimiento preventivo del hardware.

De manera general para el dominio entregar y dar soporte se proponen las siguientes buenas prácticas:

- ✓ Se recomienda definir cómo se instala y configura un equipo o un programa nuevo, cómo se documentan los cambios de los equipos y los programas, a quién se debe informar cuando hagan cambios y quién tiene la autoridad para hacer cambios de equipo, programas y configuración.
- ✓ Se recomienda que el sistema esté bien administrado y con un software de calidad, que el administrador esté al pendiente de sobre las vulnerabilidades recientes y aplicar de inmediato los parches de seguridad o actualizaciones que corrijan esos problemas.
- ✓ Es recomendable implementar apropiadamente las conexiones de red, de acuerdo con estándares y configuraciones ya probadas. Y asegurar la salida a Internet por ejemplo por

medio de firewalls diseñados con los requerimientos de los jefes. Se recomienda que al realizar el firewall se establezcan las reglas, se prohíba todo servicio, para después ir abriendo los servicios que se necesitan, tener cuidado con los puertos que se abrirán ya que pueden ser aprovechados por perpetradores. Ya implementada la red, se necesitará revisarla periódicamente, se recomienda utilizar programas de monitoreo de red, para conocer el tráfico de la red, las entradas y salidas de las peticiones de servicios.

- ✓ Para minimizar incidentes en el robo de equipos o sus componentes. Se recomienda llevar a cabo un control de los equipos, dispositivos, material que se tiene, es decir, se debe realizar un inventario de los equipos, dispositivos, componentes, entre otros. El inventario debe contener el tipo de dispositivo, fecha en que se realizó la compra, si el proveedor dio garantía.

- ✓ Se recomienda realizar una supervisión diaria de los equipos. Se debe contar con un sistema de uso del centro de cómputo, por ejemplo la elaboración de un formato que contenga el nombre de la persona, la fecha y hora en que utilizó el equipo, esto para ubicar la pérdida exacta si es el caso.

- ✓ Para un acercamiento y familiarización a las TIC's, se debe asegurar facilidad en su uso para apoyar el proceso de aprendizaje de los usuarios. Se recomienda que las tecnologías sean accesibles, es decir, contar con información e indicaciones claras y precisas de uso.
- ✓ Recomendarle a los usuarios e involucrados en el centro de cómputo, que solo utilicen el equipo para uso laboral, tareas, es decir solo temas relacionados con el trabajo.

4) MONITOREAR Y EVALUAR

a. ME1 Monitorear y evaluar el desempeño de TI

Con el propósito de tener transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TIC's.

Buenas prácticas

- ✓ Definir y establecer un enfoque del monitoreo.

- ✓ Evaluar el desempeño.

- ✓ Realizar un reporte a los directivos, encargados y administradores. (Traducir los reportes de desempeño a lenguaje directivo).

- ✓ Comparar el desempeño contra las metas acordadas.

- ✓ Identificar e implementar acciones de mejoramiento del desempeño. Realizando acciones correctivas.

b. ME2 Monitorear y evaluar el control interno

Con esto se tiene el beneficio de proporcionar seguridad respecto a operaciones eficientes y efectivas con el cumplimiento de las leyes y regulaciones aplicables.

Buenas prácticas

- ✓ Definir los sistemas de controles internos en los procesos de las TIC's.
- ✓ Monitorear, reportar y evaluar la eficiencia y la efectividad de los controles internos de las TIC's, realizando revisiones de auditoría.
- ✓ Identificar las excepciones de control y reportarlas a los encargados para tomar decisiones.
- ✓ Evaluar la efectividad de los controles llevando a cabo una auto evaluación.
- ✓ Evaluar el estado de los controles internos por medio de servicios externos.
- ✓ Identificar, iniciar, rastrear e implementar acciones correctivas.

c. ME3 Garantizar el cumplimiento regulatorio

Asegura la identificación de las leyes, regulaciones aplicables, el nivel de cumplimiento de las TIC's y la optimización de los procesos para reducir el riesgo de no cumplimiento.

Buenas prácticas

- ✓ Optimizar la respuesta a requerimientos externos.
- ✓ Evaluar el cumplimiento con los requisitos externos.
- ✓ Asegurar el cumplimiento de las políticas internas.

d. ME4 Proporcionar gobierno de TI

Este proceso tiene el propósito de elaborar informes para los directivos o responsables sobre la estrategia, el desempeño y los riesgos de las TIC's.

Buenas prácticas

- ✓ Definir y establecer las estructuras, procesos, roles y responsabilidades.
- ✓ Administrar los programas de inversión.
- ✓ Administrar los recursos.
- ✓ Administrar los riesgos.
- ✓ Medir el desempeño.

De manera general para el dominio monitorear y evaluar se proponen las siguientes buenas prácticas:

- ✓ Se recomienda colocar una computadora que vigile el tráfico en la red y sea capaz de detectar los ataques conocidos en tiempo real. Con esto se garantiza reducir la proliferación de virus informáticos en el interior del centro de cómputo (en servidores y estaciones de trabajo).
- ✓ Se debe realizar un escaneo del sistema con el antivirus instalado, configurado y actualizado, recomendablemente cada 15 días o cada mes. Y un análisis con un limpiador de registro (por programas desinstalados o programas de inicio) cada 2 meses.
- ✓ Se recomienda utilizar herramientas necesarias, como actualizaciones de sistemas operativos, antimalware, antispyware, antivirus actualizados y bien configurados.
- ✓ Se recomienda evaluar la configuración actual del hardware y software, tomando en cuenta las aplicaciones y el nivel de uso de los sistemas, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de las instalaciones.
- ✓ Se recomienda revisar periódicamente los archivos compartidos en red, así como los servicios compartidos y corroborar que únicamente tengan acceso las personas con ese privilegio.
- ✓ Se debe evaluar el desempeño y la capacidad actual de los sistemas de información en términos de la funcionabilidad, estabilidad, complejidad, costo, fortalezas y debilidades del centro de cómputo.
- ✓ Realizar una alineación entre las metas obtenidas y metas esperadas, por medio de una evaluación del personal involucrado, los sistemas, la funcionalidad, la eficiencia y el desempeño de los asesores técnicos.
- ✓ Para garantizar la disponibilidad de los equipos, se recomienda realizar exámenes periódicos a los equipos respecto a calidad en sistema y programas y en caso de existir problemas técnicos contar con sistemas alternativos que puedan colaborar en mitigar posibles fallas. Los recursos existentes deben estar para ser usados.
- ✓ Se recomienda que los administradores de red examinen la capacidad de memoria y almacenamiento máximo del sistema de cómputo para atender los procesos de todos los usuarios que se encuentran conectados a la red.
- ✓ Se recomienda contar con un equipo para realizar análisis y, recuperación de información de las unidades extraíbles, discos duros extraíbles. Este equipo debe contener distintos tipos de antivirus, antimalware, distintas herramientas para el análisis de equipos y unidades.

- ✓ Para tener seguridad en los dispositivos extraíbles. Es recomendable que se les solicite a los usuarios, que al hacer uso del equipo de cómputo e ingresar dispositivos extraíbles, deben analizar con el antivirus sus dispositivos. Ya que pueden contener software pirata, código malicioso, virus, etcétera. Que pueden ser utilizados por personas ajenas al centro de cómputo con intenciones maliciosas. Además de eliminar la opción de autoejecutable.

- ✓ Los atacantes modifican algunos archivos del sistema para asegurar que puede regresar a esa computadora cuando lo desee. Para esto se recomienda una herramienta para detectar estos casos, la verificación de la integridad de los archivos importante del sistema. El sistema de verificación debe estar protegido contra manipulación. Esta técnica es fácil de usar, económica y efectiva, que debe estar implementada en las computadoras. Al completar la información que provee la identificación de archivos modificados, sustituidos, eliminados o nuevos es posible rastrear el punto de entrada del intruso.

- ✓ Se recomienda elaborar evaluaciones, para la retroalimentación, se deben hacer en forma periódica. Se recomienda contar con un auditor de sistemas, de preferencia ajeno al centro de cómputo.

- ✓ Se recomienda evaluar el nivel de riesgo que puede tener la información en caso de pérdida, y elaborar un estudio sobre el costo que se tendría. Esto para conocer la importancia de la información y de los equipos.

- ✓ Se recomienda realizar un análisis que determine cuáles son los controles que dan un máximo de protección a un menor costo (puede haber controles que sirvan para mitigar la ocurrencia de varias amenazas). Vigilando que los controles seleccionados sigan los objetivos del centro de cómputo. Se recomienda, elaborar un reporte sobre la implementación de los controles sugeridos. El reporte debe contener:

    - Antecedentes y alcance del análisis.
    - Identificación de amenazas.
    - Determinación del factor de riesgo total.
    - Identificación de controles.
    - Análisis costo/beneficio.
    - Recomendación de controles.
    - Verificar que los controles cumplan con los objetivos requeridos.

Al finalizar la propuesta de las buenas prácticas es conveniente redactarlas en un documento o cuadernillo que contenga todas las buenas prácticas de acuerdo con su prioridad, así mismo redactar una guía rápida con los rasgos de mayor relevancia para el centro de cómputo.

A continuación se presenta un ejemplo de una guía rápida, que debe ser de fácil acceso y redactarse brevemente para que el personal involucrado tenga una lectura rápida de las buenas prácticas.

Buenas prácticas para el centro de cómputo.

- Todos los usuarios deben leer y comprender las buenas prácticas antes de tener acceso a los recursos.
- Realizar una bitácora detallando los cambios más destacados.
- Llevar un registro de acceso al centro de cómputo.
- Se recomienda determinar a los usuarios lo que se puede y lo que no se puede hacer con los equipos de cómputo, impresoras escáneres, fax, etcétera.
- Colocar un cartel con el reglamento de lo que se puede hacer y lo que no con los dispositivos.
- Proporcionar ayuda sobre el equipo y paquetería, por parte del soporte técnico a los usuarios.
- Proporcionar cursos previos sobre el manejo de equipo y paquetería instalados.
- Indicar la responsabilidad de los usuarios en la protección de la información que manejan y en qué condiciones pueden afectar o leer datos que no les pertenezcan.
- Se recomienda que los usuarios inicien sesión sin privilegios, para que solo los administradores y encargados tengan los privilegios para realizar modificaciones o instalaciones en los equipos de cómputo.
- Debe indicar si está permitido compartir cuentas de usuario, cómo se debe usar el correo electrónico, las páginas que hay en la red, entre otros.
- Se deben especificar las jerarquías de confidencialidad e integridad y cómo se implementa su protección.
- Se debe determinar quién establece los cambios de configuración del cortafuego. También quiénes deben tener acceso y quién puede obtener información del cortafuego.
- Actualizar e instalar aplicaciones secundarias, pero necesarias como java, flash y ActiveX.
- Llevar a cabo un control de calidad en productos de software.
- Se deben crear planes de recuperación de la información en caso de pérdida.
- Colocar en aplicaciones como correo electrónico, sistemas de autenticación financiera, entre otros, colocar certificados digitales.
- Monitorear la red, el tráfico de red. Llevar un control y mantenimiento para el tráfico de red.
- Promover el concepto de seguridad.

Para complementar lo antes mencionado, se debe crear conciencia de seguridad a los usuarios y a los responsables del centro de cómputo sobre la información crítica o sensible, brindándoles la información por medio de conferencias, folletos, letreros dentro del centro de cómputo, pláticas informativas.

Se debe tener en cuenta que nunca se va a poder tener un sistema perfecto y siempre se estará en riesgo de que haya intrusos que generen problemas, por ello es recomendable revisar periódicamente los equipos e instalar aplicaciones de seguridad que van a ser manejadas por especialistas en seguridad, los cuales las van a monitorear periódicamente.

6. PROMOVER EL CONCEPTO DE SEGURIDAD

Es necesario y factible, que en el centro de cómputo se promueva el concepto de seguridad, para prevenciones y detecciones de elementos no autorizados.

Se recomienda al personal de administración de la seguridad, participar en la elaboración de mensajes cortos y precisos, de conceptos como seguridad, amenazas, vulnerabilidades, ataques, riesgo, así como ejemplos de prevención y detección.

Los mensajes deben elaborarse en pequeños carteles colocados dentro del centro de cómputo.

5.2 DIFUSIÓN DE LAS BUENAS PRÁCTICAS

Para la elaboración y difusión de buenas prácticas es necesario la recopilación y difusión de experiencias positivas con el fin de retroalimentar y favorecer el aprendizaje.

La difusión de las buenas prácticas es indispensable para el desarrollo completo de la seguridad informática en el centro de cómputo. Se recomienda que participen todos los involucrados del centro de cómputo con el fin de compartir experiencias y conocer las prácticas a seguir por parte del departamento de seguridad en el centro de cómputo.

Esto para tener un buen porcentaje de seguridad, el cual proporciona un mejor manejo de datos, así como la integridad, disponibilidad de los datos y los servicios. Al difundir las buenas prácticas, se evitan incidentes y riesgos propiciados por errores o por faltas de comunicación (entre los menos graves).

Como se vio anteriormente es recomendable que todo el personal y los involucrados en el centro de cómputo conozcan el contenido de las buenas prácticas, con el fin de minimizar riesgos y propiciar la participación de todos en la seguridad del centro de cómputo.

En la difusión de las buenas prácticas, se trata de propagar, divulgar y difundir los objetivos, las metas, recomendaciones, beneficios y sanciones. Eso con el fin de crear conciencia en todo el personal del centro de cómputo, de la importancia de seguir y respetar las buenas prácticas.

Para la difusión de buenas prácticas, se recomienda exponer los casos de éxito, y redactar un documento, que contenga:

- Introducción.
- Presentación del problema.
- Solución.
- Beneficios.
- Conclusiones.

El documento que se difundirá tendrá que ser objetivo, claro, conciso y fácil de entender.

Es necesario motivar a los usuarios a seguir las buenas prácticas, entender y aprender acerca del tema. Motivándolos con programas de aprendizaje, cursos, es decir, formarles un desempeño respecto a la seguridad de la información para que comprendan la importancia de la misma y la relación que se tiene con los servicios utilizados.

También en el documento o cartel que se va a difundir, se recomienda puntualizar las ventajas, beneficios que se obtendrán al seguir las buenas prácticas, es decir, mostrar a los usuarios y a los involucrados en el centro de cómputo la parte práctica en la que se muestre la eficiencia de esta estrategia, para proteger los activos de los usuarios y los del centro de cómputo, así como los servicios proporcionados.

Al difundir se divulga la información y el crecimiento acerca de las buenas prácticas, con el propósito de acercar temas de seguridad a los usuarios de manera práctica, con el objetivo de motivar a los usuarios y personal del centro de cómputo para que se capaciten constantemente, se respete y se promueva el uso de las buenas prácticas en todo momento, dentro y fuera del centro de cómputo.

Con base en lo investigado, para realizar la difusión de las buenas prácticas se recomienda lo siguiente:

a) Elaboración de carteles

Es necesario para la difusión de las buenas prácticas elaborar carteles que contengan las recomendaciones con ilustraciones, esto para tener la mayor atención posible por parte de los usuarios. Para informar a usuarios y personal involucrado acerca de las recomendaciones por parte de los administradores de seguridad y la dirección del centro de cómputo.

Ejemplo de la recomendación de análisis con antivirus y otras aplicaciones. (Figura 5.3)

Figura 5.3 Análisis con antivirus y otras aplicaciones

Colocar a la vista los carteles de las buenas prácticas para su uso adecuado en el centro de cómputo, con mensajes cortos para que sean de lectura rápida.

Este tipo de difusión, son complemento de ayuda para captar la atención de los usuarios con el fin de que se interesen más por la seguridad de su información y de la seguridad que les brinda los servicios del centro de cómputo.

b) Elaboración de trípticos

Otra manera de difundir la información y hacer llegar el concepto de seguridad a los usuarios y personas involucradas en el centro de cómputo es la elaboración de trípticos con información sobresaliente de buenas prácticas, algunos ejemplos de interés y algunas páginas de internet para consultar y saber más del tema.

c) Recomendación o elaboración de páginas de internet especializadas en el tema.

Proporcionar o brindarle a los usuarios, recomendaciones de páginas referentes a la seguridad en cómputo. Páginas donde se publiquen vulnerabilidades, blogs de seguridad, páginas de interés, por ejemplo de curso, diplomados. Si los encargados así lo deciden, elaborar una página referente a temas de seguridad, políticas de seguridad, buenas prácticas, etcétera.

Por ejemplo:

- http://www.tic.unam.mx/
- http://www.segu-info.com.ar

d) Conferencias, cursos y diplomados.

Al capacitar a los administradores, técnicos y demás personal involucrado en la seguridad del taller de cómputo es una forma de propagar la información, ya que por medio de su conocimiento e interés, los usuarios se van a ir involucrando más en la seguridad, al ser orientados por ellos y propiciar que conozcan más herramientas para brindarle seguridad a su información. Y con su ayuda brindarle seguridad a los servicios del centro de cómputo.

Con esto se pretende proporcionar a los usuarios, información de las ventajas que brinda implementar la seguridad en el centro de cómputo. Con el principal propósito que se involucren, entiendan y participen en colaboración con los involucrados, para tener un centro de cómputo más seguro y para que se les brinde un servicio confiable. Teniendo grandes ventajas para ellos como por ejemplo, mantener su información libre de pérdida o modificación debido a la intrusión.

También con el propósito de que los involucrados y los usuarios, se capaciten y se sientan motivados para conocer las políticas, buenas prácticas e información de las nuevas TI. Continuando con el ciclo de las buenas prácticas de: Analizar, plantear, difundir, actualizar y retroalimentar las buenas prácticas de seguridad en el centro de cómputo.

ACTUALIZAR Y RETROALIMENTAR LAS BUENAS PRÁCTICAS POR PERIODOS CORTOS

Hay que tener en cuenta que hasta con el personal más capacitado o expertos en seguridad y con herramientas de última generación habrá fugas o se cometerán errores, ya que es imposible una seguridad al 100%. Siempre existirán fallas que en su momento tendrán que ser analizadas y cuestionadas y ajustadas para desarrollar una solución que se adecúe a las nuevas necesidades.

Por ello, es necesario llevar a cabo una revisión periódica de al menos 6 meses, para realizar cualquier modificación de nuevas tecnologías, amenazas encontradas, lo que no se haya considerado en la anterior elaboración de buenas prácticas y mitigar esos riesgos.

Al actualizar las buenas prácticas se van llenando los agujeros no considerados anteriormente, con esto disminuye la posibilidad de intrusión. En cualquier tipo de sistema de seguridad nunca se debe confiar de que se cuenta con un sistema seguro, por eso aunque todo marche bien se deben realizar revisiones periódicas y realizar las modificaciones, actualizando lo antes posible el documento oficial, así como en las formas de difusión (si es el caso).

CONCLUSIONES

Las buenas prácticas proporcionadas en este trabajo de acuerdo con la experiencia y con base en el marco de trabajo de COBIT, son el resultado de una investigación para brindar a los lectores una base para la administración de la seguridad en un centro de cómputo.

Proporcionando métodos y estrategias para la elaboración, implementación, retroalimentación y difusión de las buenas prácticas de seguridad con el fin de optimizar los recursos del centro de cómputo.

Es importante enfatizar que se tiene que concientizar a los involucrados, brindándoles políticas de seguridad y buenas prácticas, también ayudándolos con cursos de capacitación donde se proporcione información necesaria y conceptos relacionados con la seguridad de la información que se puedan poner en práctica.

Es necesario hacer énfasis en realizar actualizaciones en equipos, software, políticas y buenas prácticas, debido a que cualquier organización va cambiando conforme pasa el tiempo, es menester recordar que la protección y prevención de los activos radica en el ciclo de la seguridad (planear, hacer, verificar y actuar). También resulta de gran importancia identificar las consecuencias que se tendrán si se pierde información confidencial, esto para ayudar a prevenir posibles incidentes y tener un alto grado de seguridad.

Es importante resaltar que es conveniente reconocer las vulnerabilidades del entorno de trabajo e identificar las amenazas que podrían atentar contra la información, examinando periódicamente si el entorno de trabajo es “seguro”, todo ello para proporcionar un buen esquema de buenas prácticas, respecto a los requerimientos diarios de los usuarios y administradores del centro de cómputo.

Este trabajo tendrá continuidad para las organizaciones, mejorar la administración y el uso del centro de cómputo, dando seguimiento diario a su inventario del hardware, dar mantenimiento preventivo al equipo, proporcionar recomendaciones sobre el mejor uso del lugar, mejorar el control de acceso, actualizar y mejorar periódicamente las medidas de seguridad en la administración de la red.

Es preciso resaltar que al elaborar, evaluar y retroalimentar las políticas de seguridad en el centro de cómputo, así como identificar y entender por qué son importantes las políticas de seguridad y las buenas prácticas, se obtiene como resultado mejorar la confidencialidad, integridad y disponibilidad mediante la implementación de controles y recomendaciones que se deben seguir en todo momento.

Agregando una última recomendación, hasta con el personal más capacitado y con la tecnología más reciente, se debe considerar que siempre habrá fugas o huecos en la seguridad ya que es imposible una seguridad al 100%, siempre existirán fallas que en su momento tendrán que ser analizadas, cuestionadas y ajustadas para desarrollar una solución. Teniendo en cuenta que es posible brindar altos grados en seguridad, es por ello que se debe concientizar a los involucrados y

preparar el centro de cómputo con los servicios necesarios que se brindarán, para esto es necesario contar con sus respectivas políticas y buenas prácticas.

Este trabajo sirve como base en la elaboración de las buenas prácticas para los centros de cómputo en México, ya sea desde un centro de cómputo de consulta, docente, administrativo hasta de tipo empresarial.

También tiene el propósito de identificar la forma más óptima para resguardar la información, identificando los activos, conocer su prioridad respondiendo a las preguntas indispensables: ¿qué se quiere proteger?, ¿de qué se quiere proteger? y ¿cómo se va a proteger?

Otro propósito es realizar un análisis de las metas u objetivos cumplidos o esperados al prestar servicios en el centro de cómputo y con base en eso proponer nuevos objetivos para mejorar el servicio a los usuarios.

Sin dejar en segundo término el análisis de las prácticas utilizadas diariamente para tener una base y con ello poder identificar, evaluar y diseñar nuevas prácticas para el centro de cómputo, incrementando así el nivel de seguridad existente.

La finalidad es aplicar las recomendaciones para el buen uso del centro de cómputo, para esto es necesario considerar las buenas prácticas presentadas en este trabajo lo antes posible para que no se vea afectada la información. Iniciando y fomentando la importancia de las buenas prácticas entre todos los involucrados acerca de la seguridad informática y de la información.

GLOSARIO DE TÉRMINOS

ADMINISTRACIÓN

Es el empleo de la autoridad para organizar, dirigir y controlar subordinados responsables, con el fin de que todos los servicios que se presentan sean debidamente coordinados en el logro del fin de la empresa.

AES

Advanced Encryption Standard – Estándar de cifrado Avanzado. Es un esquema de cifrado por bloques, usado en la criptografía simétrica.

ARP

Address Resolution Protocol - Protocolo de resolución de direcciones. Es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (MAC address para Ethernet) que corresponde a una determinada dirección IP.

ANÁLISIS DE RIESGOS

Es una evaluación de amenazas y vulnerabilidades de la información y su impacto en el procesamiento de la información así como su probabilidad de ocurrencia.

ANTISPYWARE

Antispyware - Anti-espía. Es un programa o aplicación de seguridad, que se dedica especialmente a la protección de la información en la computadora de los programas espías, eliminando los riesgos de infección. Esta aplicación verifica y elimina lo que no pertenece al sistema y que puede robar información sin que se den cuenta.

ANTIMALWARE

Antimalware – Anti-software malicioso. Es un programa o aplicación, que escanea todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza. Proporciona protección en tiempo real, detectando y eliminando malware. Los programas anti-malware escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en la computadora. Al terminar el escaneo muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuáles eliminar.

AMENAZAS

Todo aquello que intenta o pretende destruir, es un peligro latente que puede dañar y que puede llegar a culminarse o puede no hacerlo. Una amenaza será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Puede causar alteraciones a la información, ocasionándole pérdidas materiales, económicas, de información y de prestigio.

AUDITORÍA

Es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado. Es decir, es la evaluación de la eficiencia y eficacia con que se está operando para tomar decisiones con el fin que permitan corregir los errores o bien mejorar la forma de actuación.

BUENAS PRÁCTICAS

Las buenas prácticas son recomendaciones o consejos que se le dan al personal durante su trabajo o al momento de su capacitación, para que éste desarrolle de manera eficiente el trabajo, resuelva o evite problemas relacionados con las actividades a realizar. Las cuales surgen de la experiencia y se apoyan en algunas políticas de seguridad de la misma organización.

CIA (CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD)

Confidentiality, Integrity, Availability - Confidencialidad, disponibilidad e integridad. Conocida como la tríada CIA. Son los principios básicos de la seguridad de la información, compuesta por la confidencialidad, disponibilidad e integridad.

4. Confidencialidad.- Condición que garantiza que la información es accedida sólo por las personas autorizadas según la naturaleza de su cargo o función dentro de la organización.
5. Integridad.- Condición que garantiza que la información es consistente o coherente.
6. Disponibilidad.- Condición que garantiza que la información puede ser accedida en el momento en que es requerida.

COBIT

Objetivos de Control para la Información y las Tecnologías Relacionadas - Control Objectives for Information and related Technology. Es un conjunto de herramientas de apoyo que permite a los administradores a reducir la brecha entre las necesidades de control, cuestiones técnicas y riesgos de negocio.

CYBERBULLING

Cyberbullying - Ciberacoso. Es el uso de información electrónica y medios de comunicación (correo electrónico, redes sociales, blogs, mensajes de texto, teléfonos móviles, y websites difamatorios) para acosar a un individuo o grupo, mediante ataques personales u otros medios. Pretendiendo causar angustia emocional y preocupación.

DAFO

El análisis DAFO es también conocido como FODA.

DHCP

Dinamic Host Configuration Protocol - Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (configuración de red) en forma dinámica (es decir, sin intervención particular). Permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. El objetivo principal es simplificar la administración de la red distribuyendo direcciones IP en una red.

DMZ (ZONAS DESMILITARIZADAS)

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. Las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna.

DNA

Abreviatura de ácido desoxirribonucleico - DNA. Es la molécula que contiene y transmite la información genética de los organismos.

DNS

Domain Name System - *Sistema de nombres de dominio.* Conjunto de protocolos y servicios, que contiene una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Relacionando las IP's con los nombres canónicos (http://132.248.54.13/) y los alias (http://www.ingenieria.unam.mx/).

ESSID/SSID

ESSID (Extended Service Set IDentifier). Es utilizado en las redes en infraestructura que incorporan un punto de acceso. *SSID (Service Set IDentifier)* Es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

FINGERPRINTING

Fingerprinting - Identificación por huella dactilar. Es la identificación por medio de huellas digitales o de los dedos. El fingerprinting es una técnica que cosiste en analizar las huellas que deja un sistema operativo en sus conexiones de red.

FIREWALL

Un firewall es un dispositivo que tiene un conjunto de reglas específicas, con las cuales determina qué tráfico de red entra o sale de la red. Generalmente es usado para interconectar una red privada con Internet, también se utiliza para implementar controles de acceso al interior de la red.

FODA

Es una metodología de estudio de la situación de una empresa o un proyecto, analizando sus características internas (Debilidades y Fortalezas) y su situación externa (Amenazas y Oportunidades).

GPRS (General Packet Radio Service)

General Packet Radio Service - Servicio general de paquetes vía radio. Es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos mediante conmutación de paquetes. Se pueden utilizar servicios como Wireless Application Protocol (WAP), servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS), Internet y para los servicios de comunicación, como el correo electrónico y la World Wide Web (WWW).

GSM (Global System for Mobile Communication)

Global System for Mobile communications - Sistema global para las comunicaciones móviles. Es un sistema estándar, libre regalías, de telefonía móvil digital. Un cliente GSM puede conectarse a través de su teléfono con la computadora, enviar y recibir mensajes por correo electrónico, faxes, navegar por Internet, así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS) o mensajes de texto.

HIDS

Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en un host. Puede tomar medidas protectoras.

IDS

Los IDS tienen dos categorías principales, los que son basados en host (HIDS) y de red (NIDS).

IDS - Sistemas Detectores de Intrusos. Este tipo de sistema detecta tráfico malicioso en la red. Escucha el tráfico de manera promiscua, monitorea los paquetes en la red y alerta si hay una actividad maliciosa. Además detectan gran cantidad de tipos de ataques. Los IDS no están en la red, si se quita el IDS, el flujo de la red continúa.

IEEE

Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos. Es una asociación técnico-profesional mundial dedicada a la estandarización.

INFORMACIÓN

Es un conjunto de datos que tienen un significado para alguien o algo.

INTERRUPCIÓN

Es una suspensión temporal de la ejecución de un proceso.

INTERCEPCIÓN

Acción y efecto de interceptar. Se refiere a detener algo en su camino; interrumpir una vía de comunicación o apoderarse de algo antes de que llegue a su destino.

INTERNET

Es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.

IP

Protocolo de Internet. Se encuentra en la capa de red. Este protocolo contiene información de direccionamiento y alguna información de control para habilitar paquetes para ser enviados a la mejor ruta (routing) en una red. Es un identificador único que ayuda a localizar la ubicación de una computadora en la red.

IPS

Sistemas Preventores de Intrusos. Este sistema bloquea tráfico malicioso durante el mismo flujo de la información. Forma parte de la estructura de la red. Disminuye la actividad administrativa para su mantenimiento. El IPS está en la red, si se quita el IPS no hay flujo de red.

kbps

Kilo Bits por Segundo. Es una unidad de medida de información, utilizada para medir el tráfico de la información por un canal digital que se transfieren de un punto a otro en un segundo.

MAC

Media Access Control - Control de acceso al medio. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits).

MAGERIT

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Se enfoca en el desarrollo de un proyecto de análisis y gestión de riesgos que se compone de tres grandes pasos: planificación, análisis y gestión.

MALWARE

Código maligno, software malicioso o software malintencionado. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

mbps

Millones de bits o Megabits por segundo. Es un sistema de medición de la anchura de banda.

MECANISMOS 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.

MODIFICACIÓN

Es cambiar o transformar algo, dar un nuevo modo de existencia a algo de manera que se distinga de lo que era.

MP3

Moving Picture Experts Group (MPEG). MPEG-1 Audio Layer III o MPEG-2 Audio Layer III. Es un formato de audio que combina la calidad de sonido y poco tamaño. Para conseguir un menor tamaño de archivo, el formato MP3 redujo el tamaño de los archivos de música sin casi perder la calidad por la compresión.

NIDS

NIDS - Sistema de detección de intrusiones basado en red. Se utiliza para monitorizar y analizar el tráfico de red para proteger un sistema contra las amenazas basadas en la red.

OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation - Evaluación operacional crítica de amenazas, activos y vulnerabilidades. Es una metodología de planeación y evaluación basada en riesgos. Es una metodología para la gestión de riesgos.

ORGANIZACIÓN

Es la aplicación de un conjunto de técnicas convenientes para obtener una empresa estructurada, con la correspondiente división y coordinación de las actividades. En la organización se adecúan los recursos previstos en la planificación para conseguir los objetivos.

OUTSOURCING

Outsourcing - La subcontratación, externalización o tercerización. Es el proceso económico en el cual una empresa mueve o destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato.

PDCA (PLANIFICAR, HACER, VERIFICAR, ACTUAR)

PDCA (plan-do-check-act) – Ciclo PDCA (planear-hacer-revisar-actuar). Es una estrategia de mejora continua de calidad. Enseña a las organizaciones a planear una acción, hacerla, revisarla para ver cómo se conforma al plan y actuar en lo que se ha aprendido.

PDA

Personal digital assistant - Asistente digital personal. Es un organizador personal o una agenda electrónica de bolsillo, diseñada como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

PHARMING

Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta.

PHISING

Es un término informático que denomina un tipo de abuso informático y que se comete mediante 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).

POLÍTICAS

La políticas son una serie de normas, reglamentos y protocolos por seguir, donde se definen las distintas medidas que se van a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su funcionamiento.

POLÍTICA DE SEGURIDAD

La política de seguridad es un 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 informática dentro de la misma.

P2P

Peer-to-peer - Par a par o de punto a punto. Esta tecnología es una red informática entre iguales, se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Las redes P2P, aprovechan, administran y optimizan el uso de banda ancha que acumulan de los demás usuarios en la red por medio de la conectividad entre los mismos usuarios, obteniendo más rendimiento en las conexiones y transferencias.

ROUTERS

El router es un dispositivo de seguridad, el cual se utiliza como la primera capa de protección en una arquitectura de seguridad general, es como un dispositivo de análisis. El router se encarga de dirigir el tráfico interno y externo de la red.

SCAM

Estafa. Se emplea para referirse a una red de corrupción. Se usa para definir los intentos de estafa a través de un correo electrónico fraudulento (o páginas web fraudulentas).

SEGURIDAD

Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer, todo está bien.

SERVICIOS 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.

SGC (SISTEMAS DE GESTIÓN DE CALIDAD)

Es una estructura operacional de trabajo, bien documentada e integrada a los procedimientos técnicos y gerenciales, para guiar las acciones de la fuerza de trabajo, la maquinaria o equipos, y la información de la organización de manera práctica y coordinada que asegure la satisfacción del cliente y bajos costos para la calidad.

SHARED KEY

SKA - Autenticación de clave compartida. Es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice. Se utiliza en cifrado Wi-Fi como WEP o WPA, donde tanto el punto de acceso inalámbrico (AP) como todos los clientes comparten la misma clave.

SIM O GSM

Subscriber identity module - Módulo de identificación de abonado. Es una tarjeta inteligente desmontable usada en teléfonos móviles y módems que se conectan al puerto USB. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red. El uso de la tarjeta SIM es obligatorio en las redes GSM.

SITES

Es un lugar o sitio. Se puede expresar como un punto en Internet con una dirección única a la cual acceden los usuarios para obtener información.

SPAM

Son mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

SUPLANTACIÓN

Ocupar el lugar de otra persona ilegalmente o hacerse pasar por ella contra su voluntad para obtener un beneficio.

TCI (TARJETA CON CIRCUITO INTEGRADO)

Tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI). Es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada.

TIC's

TIC's - Tecnologías de la información y la comunicación. Son el conjunto de tecnologías desarrolladas para gestionar, procesar, almacenar, recuperar y transmitir información de un lugar a otro. Principalmente de informática, internet y telecomunicaciones.

TCP

Transmission Control Protocol - Protocolo de Control de Transmisión. Es un protocolo de capa de transporte orientado a conexión. Brinda datos confiables.

TCPDUMP

Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red, a la cual la computadora está conectada.

TDES

Triple Data Encryption Standard – Estándar de cifrado de Datos Triple. Es un estándar de cifrado de calidad. Método para cifrar la información, para agrandar la clave. Es utilizada en la mayoría de las tarjetas de crédito y otros medios de pago electrónicos.

TI

TI - Tecnología de la información. Son aquellas herramientas y métodos 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).

UDP

Protocolo de datagrama de usuario. Es el protocolo de transporte no orientado a conexión de la pila de protocolo TCP/IP. Es un protocolo que intercambia datagramas sin acuse de recibo ni entrega garantizada.

UMTS (Universal Mobile Telecommunication System)

Universal Mobile Telecommunications System - Sistema universal de telecomunicaciones móviles. Es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM.

USB

Universal Serial Bus - bus universal en serie BUS. Es un estándar industrial que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras y periféricos y dispositivos electrónicos.

VERTICILOS

Se denomina verticilo a los dibujos en la huella dactilar, porque en muchos casos son similares a las flores.

VPN (REDES PRIVADAS VIRTUALES)

VPN - Redes Privadas Virtuales. Esta red es virtual porque conecta dos redes físicas (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden ver los datos.

VULNERABILIDAD

Es una debilidad que puede ser explotada para violar la seguridad.

WEP

Wired Equivalent Privacy - Privacidad Equivalente a Cableado. Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

WIMAX

Worldwide Interoperability for Microwave Access - Interoperabilidad mundial para acceso por microondas. Es una tecnología que permite la recepción de datos por microondas y retransmisión por ondas de radio.

WLAN (RED INÁLAMBRICA DE ÁREA LOCAL)

Una red inalámbrica WLAN es una red que cubre un área equivalente a la red local de una organización con un alcance aproximado de 100 metros. Esta red permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

WLL

Wireless local loop - Bucle local inalámbrico. Es el uso de un enlace de comunicaciones inalámbricas para ofrecer servicios de telefonía e Internet de banda ancha a los usuarios.

WPA (WIFI PROTECTED ACCESS – ACCESO WIFI PROTEGIDO)

Wifi Protected Access – Acceso Wifi Protegido. Cifrado de la transmisión para emitirse en un entorno seguro.

WPAN (RED INALÁMBRICA DE ÁREA PERSONAL)

Red Inalámbrica de Área Personal. Este tipo de red inalámbrica de corto alcance abarca pocos metros, esta red se utiliza para conectar dispositivos periféricos, por ejemplo, impresoras, teléfonos móviles.

ANEXO A.

Objetivos de Control para Información y Tecnologías Relacionadas - Control Objectives for Information and related Technology (COBIT)

El actual entorno económico y de competencia, los CTI (Centros de Tecnología de la Información) se caracterizan por el uso intensivo de la información y conocimiento.

A medida que se trabaja en el ámbito de la seguridad de la información y la seguridad informática, aumenta la necesidad de difundir la educación en estos temas; sin embargo en espacios laborales o educativos no es tan simple. Por ello es necesario buscar guías y documentos para abordar la seguridad de una forma responsable, procedimental y orientada al cumplimiento de los estándares mínimos requeridos para la tecnología actual.

Para garantizar el éxito en la gestión de la información, se toman en cuenta los estándares para su seguridad. Con esto se protege la información y se garantiza la implantación de las estrategias que propician la triada de la seguridad.

Los estándares y regulaciones, definen la calidad de construcción. Establecen una base para comparar, medir o juzgar la cantidad, capacidad, valor, calidad, desempeño, límites e interoperabilidad.

Un estándar es un documento con un contenido de tipo técnico-legal que establece un modelo o norma que refiere lineamientos a seguir para cumplir una actividad o procedimientos. Se recomienda su uso ya que se pretende que los procesos y actividades de organizaciones y sus personas sean organizados y estructurados. Los estándares internacionales son producto de diferentes organizaciones, para uso interno y externo.

Por ejemplo, entidades como la ISO (International Standard Organization) y la IEEE (Institute of Electrical and Electronics Engineers), entre otras proponen estos documentos, los cuales se crean a partir de la experiencia de diferentes grupos que participan durante el proceso y al finalizar estos documentos son de tipo público.

Algunos estándares internacionales, guías y manuales de buenas prácticas, que en la actualidad son empleados para buscar el aseguramiento de la información.

El seguimiento de los documentos y guías permiten en conjunto una creación de políticas y procedimientos que establecen controles de seguridad para la información y los activos asociados, brindando protección desde lo procedimental hasta lo técnico dentro de la organización, ofreciendo confianza a nivel interno y externo.

COBIT

Objetivos de Control para Información y Tecnologías Relacionadas-Control Objetives for Infornation and related Technology.

COBIT es una marca registrada de ISACA (Information Systems Audit and Control Association-Asociación de Auditoría y Control de Sistemas de Información), la cual está comprometida con el desarrollo, la adopción y uso de conocimiento y prácticas líderes en la industria de TI. También patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

La misión de COBIT es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio y profesionales de TI.

En los objetivos de control para la Información y la tecnología, COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos; brindando así la calidad, gestión y correcta administración en los servicios prestados, abordando también, temas de seguridad asociados a los servicios.

Estas prácticas ayudan a optimizar las inversiones habilitadas por TI, aseguran la entrega del servicio y brindan una medida de seguridad. Para que TI tenga éxito en satisfacer los requerimientos, se debe implementar un sistema de control interno o un marco de trabajo.

El marco de trabajo de control COBIT contribuye de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio.
- Organizando las actividades de TI en un modelo de procesos.
- Identificando los principales recursos de TI a ser utilizados.
- Definiendo los objetivos de control gerenciales a ser considerados.
- Alineación de TI con el negocio.
- Habilitar TI y maximizar los beneficios.
- Uso responsable de los recursos de TI.
- Administración de los riesgos de TI.

La orientación que enfoca COBIT consiste en alinear las metas del negocio con las metas de TI brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

Algunos de los beneficios de implementar COBIT como marco de referencia sobre TI incluye:

- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Entendimiento compartido entre todos los interesados, con base en un lenguaje común.
- Mantener información de alta calidad para apoyar las decisiones de la empresa.
- Lograr la excelencia operativa a través de una aplicación fiable y eficiente de la tecnología.
- Mantener los riesgos relacionados a TI bajo un nivel aceptable.

- Optimizar los servicios.
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.

El marco de trabajo de COBIT tiene características principales: de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones. (Figura A.1)

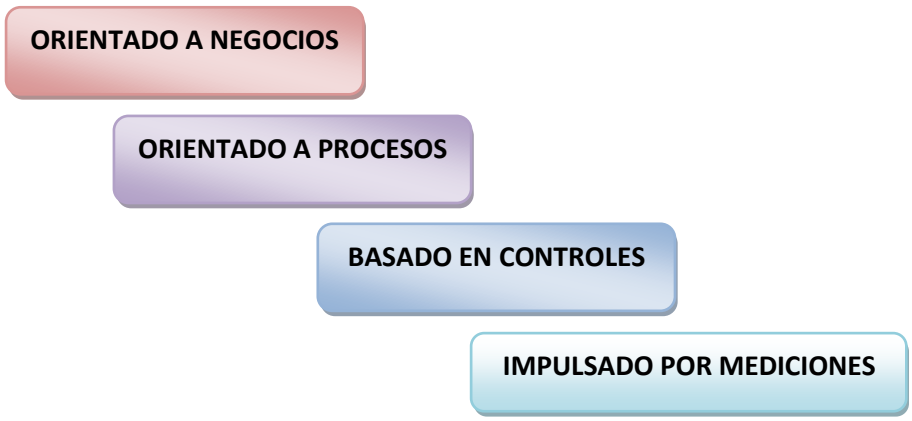

Figura A.1 Marco de trabajo de COBIT

❖ **ORIENTADO AL NEGOCIO**

Sirve como guía para los dueños del CTI, es utilizado por proveedores de servicios, usuarios y auditores de TI. Para lograr sus objetivos, la empresa necesita invertir en administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que administren los servicios. (Figura A.2)

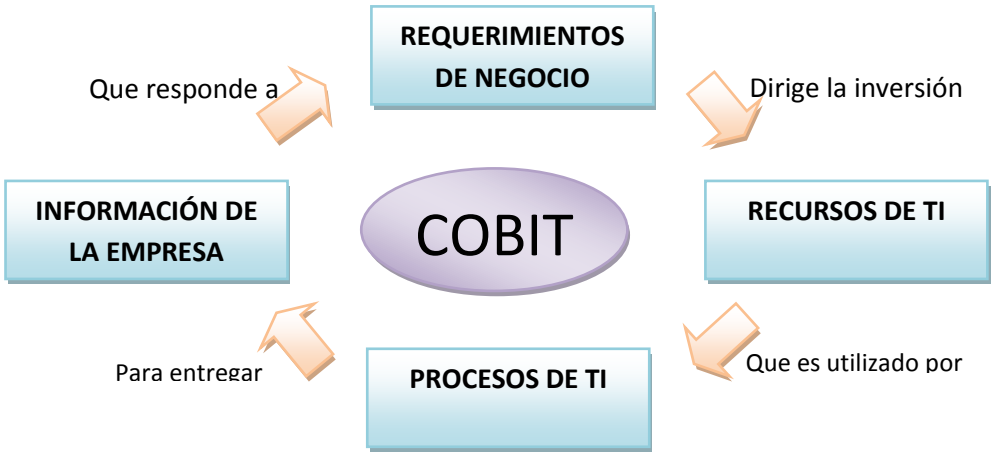

Figura A.2 Principio básico de COBIT

El marco de trabajo de COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

CRITERIOS DE INFORMACIÓN DE COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, éstos son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad y de seguridad, se definen siete criterios de información:

1. Efectividad. Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio y se proporcione de una manera oportuna, correcta, consistente y utilizable.
2. Eficiencia. Consiste en que la información sea generada optimizando los recursos.
3. Confidencialidad. Se refiere a la protección de información contra revelación no autorizada.
4. Integridad. Está relacionada con la precisión y completitud de la información.
5. Disponibilidad. Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.
6. Cumplimiento. Tiene que ver con acatar leyes, reglamentos y acuerdos, es decir, criterios de negocios impuestos externamente, así como políticas internas.
7. Confiabilidad. Se refiere a proporcionar la información apropiada para que se administre la entidad y ejerza sus responsabilidades.

Una vez que han sido definidas las metas alineadas, éstas requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas.

RECURSOS DE TI

- Las aplicaciones incluyen sistemas de usuario automatizados y procedimientos manuales que procesan información.
- La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información.
- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etcétera, así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

❖ **ORIENTADO A PROCESOS**

Se definen las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios: planear y organizar, adquirir e implementar, entregar y dar soporte, monitorear y evaluar (Figura A.3). Un modelo de procesos, permite que se definan las responsabilidades.

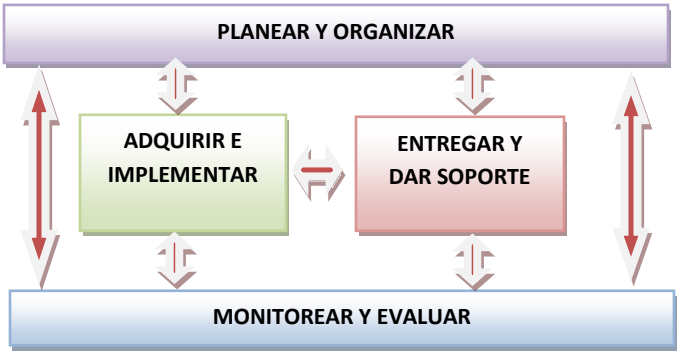

Figura A.3 Los cuatro dominios interrelacionados de COBIT

Estos dominios son:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. La realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Este dominio cubre lo siguiente:

- Alineación de las estrategias de TI y del negocio.
- Se optimizan los recursos.
- Se entienden y administran los riesgos de TI.

ADQUIRIR E IMPLEMENTAR (AI)

Las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas en los procesos del negocio. El cambio y el mantenimiento de los sistemas existentes, garantiza que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, cubre lo siguiente:

- Se realiza un trabajo adecuado con los nuevos sistemas, una vez implementados.
- Los cambios no afectan a las operaciones actuales del negocio.

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Por lo general cubre lo siguiente:

- Entrega de los servicios de TI de acuerdo con las prioridades del negocio.
- Optimizar los costos de TI.
- Utilizar los sistemas de TI de manera productiva y segura.
- Implementadas de forma adecuada la confidencialidad, la integridad y la disponibilidad.

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación. Por lo general abarca lo siguiente:

- Mide el desempeño de TI para detectar los problemas.
- Garantiza que los controles internos son efectivos y eficientes.
- Mide y reporta los riesgos, el control, el cumplimiento y el desempeño.

❖ **BASADO EN CONTROLES**

Con las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad en los objetivos de negocio, los eventos no deseados serán prevenidos o detectados y corregidos. Se lleva a cabo el control, comparando las normas y estándares con la respuesta de los procesos revisando que se estén cumpliendo y llevando un control de los riesgos obtenidos.
Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia, debido a que habrá menos errores y un enfoque de administración más consistente.

CONTROLES DEL NEGOCIO Y DE TI

El sistema de control interno de la empresa impacta en TI a tres niveles

- Nivel de dirección ejecutiva
  Se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía.

- Nivel de procesos de negocio
  Los controles al nivel de procesos de negocio son una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.

- Controles generales de TI
  Mucha de la infraestructura de TI provee un servicio común (es decir, redes, base de datos, sistemas operativos y de almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación.

CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

Los controles generales son aquellos que están inmersos en los procesos y servicios de TI. Por ejemplo:

- Desarrollo de sistemas.
- Administración de cambios.
- Seguridad.
- Operaciones de cómputo.

Los controles incluidos en las aplicaciones de los procesos del negocio se conocen como controles de aplicación. Por ejemplo:

- Integridad.
- Precisión.
- Validez.
- Autorización.
- Segregación de funciones.

La responsabilidad operativa de administrar y controlar los controles de aplicación es una responsabilidad conjunta, entre el negocio y TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

La empresa es responsable de:

- Definir apropiadamente los requisitos funcionales y de control.
- Uso adecuadamente de los servicios automatizados.

TI es responsable de:

- Automatizar e implementar los requisitos de las funciones de negocio y de control.
- Establecer controles para mantener la integridad de controles de aplicación.

Los procesos de TI de COBIT abarcan los controles generales de TI, sólo los aspectos de desarrollo. En los controles de aplicación, la empresa es responsable de definir el uso operativo. (Figura A.4)

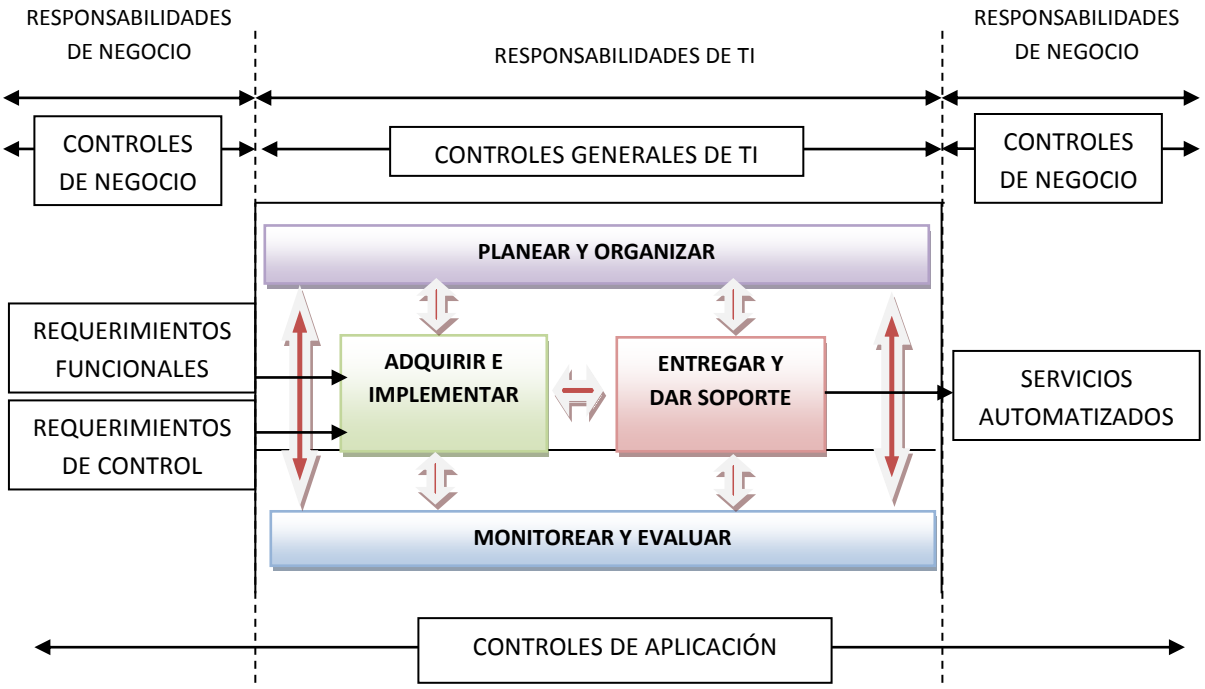

Figura A.4 Fronteras de los controles de negocio, generales y aplicación

❖ **IMPULSADO POR LA MEDICIÓN**

Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. COBIT atiende estos temas a través de:

MODELOS DE MADUREZ

En este modelo se debe considerar el equilibrio del costo beneficio. Para conocer qué tan bien está administrado TI se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información.

Los niveles de madurez están diseñados como perfiles de procesos de TI, que se reconocen como descripciones de estados posibles actuales y futuros.

Utilizando los modelos de madurez se puede identificar:

- El desempeño real de la empresa. (¿Dónde se encuentra la empresa hoy?)
- El estatus actual de la industria. (La comparación)
- El objetivo de mejora de la empresa. (¿Dónde desea estar la empresa?)
- El crecimiento requerido entre “cómo es” y “cómo será”

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, desde un nivel de no-existe (0) hasta un nivel optimizado (5). (Figura A.5)

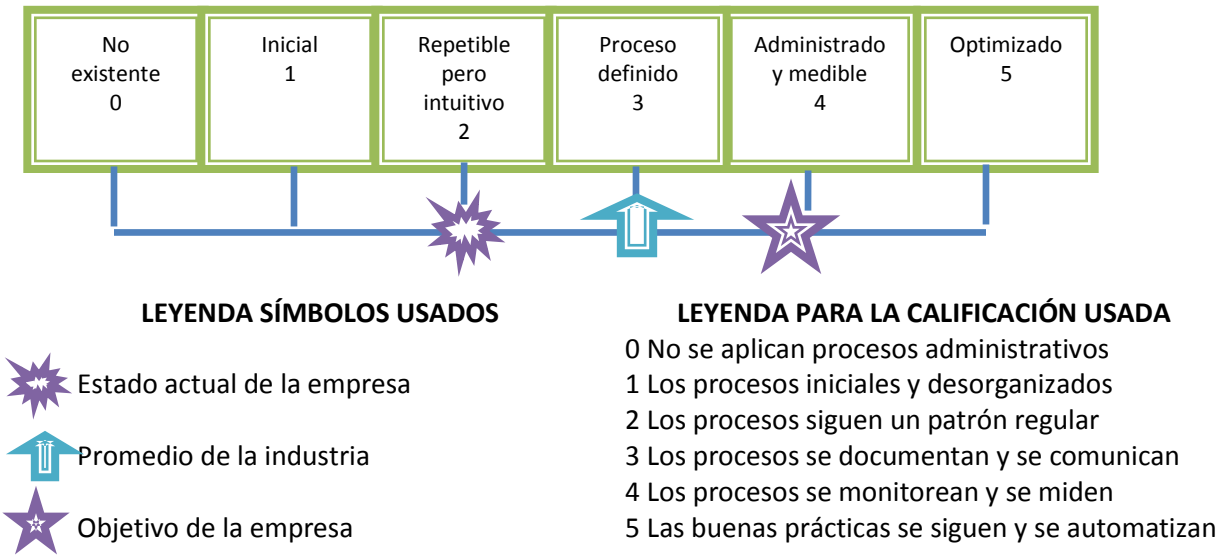

Figura A.5 Representación gráfica de los Modelos de Madurez

A continuación se presenta el modelo genérico de madurez.

a) *0 No existe.* Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver

b) *1 Inicial.* Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo, no existen procesos estándares en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

c) *2 Repetible.* Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

d) *3 Definido.* Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

e) *4 Administrado.* Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

f) *5 Optimizado.* Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

La ventaja de un modelo de madurez es ubicarse en la escala a evaluar, qué se debe hacer si se requiere desarrollar una mejora. Una empresa debe analizar los controles necesarios

para asegurar que el riesgo sea mitigado y que se obtenga el valor de acuerdo con los objetivos del negocio. Las escalas del modelo de madurez ayudan a explicar a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran.

A los modelos de madurez se añaden, algunos principios contenidos en los siguientes atributos, a través de niveles:

- Conciencia y comunicación.
- Políticas, estándares y procedimientos.
- Herramientas y automatización.
- Habilidades y experiencia.
- Responsabilidad y rendición de cuentas.
- Establecimiento y medición de metas.

A continuación se presenta la tabla de atributos de madurez (Tabla A.1), es una lista de características de cómo se administran los procesos de TI y describe cómo evolucionan desde un proceso no existente hasta uno optimizado.

a)

CONCIENCIA Y COMUNICACIÓN	POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS	HERRAMIENTAS Y AUTOMATIZACIÓN
1 Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos.	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas.
2 Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de políticas y procedimientos.	Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.
3 Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.	Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado.
4 Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.
5 Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación.	Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.	Se usan juegos de herramientas estandarizados a lo largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora de los procesos y automáticamente detectar excepciones a los controles.

Tabla de atributos de madurez (Tabla A.1)

b)

HABILIDADES Y EXPERIENCIA	RESPONSABILIDADES Y RENDICIÓN DE CUENTAS	ESTABLECIMIENTO Y MEDICIÓN DE METAS
No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal	No existe definición de responsabilidades y rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	Las metas no están claras y no existen las mediciones.
Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	Existen algunas metas; se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.
Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos del negocio.	Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de codo consistente.
Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la compartición del conocimiento.	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar responsabilidades. Existe una cultura de recompensas que activa la acción positiva.	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI.
La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y se están desarrollando sistemas basados en el conocimiento. Expertos externos y líderes industriales se emplean como guía.	Los dueños de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz.

Un ambiente de control implantado de forma adecuada, se logra cuando se han conseguido los tres aspectos de madurez (capacidad, desempeño y control). El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.

MEDICIÓN DEL DESEMPEÑO

La medición del desempeño, es esencial para determinar cuál es el desempeño real de la empresa en sus procesos de TI. Las metas de TI ayudan a definir las diferentes metas de procesos. Las métricas y las metas se definen en COBIT a tres niveles:

- Las metas y métricas de TI que definen lo que el negocio espera de TI.
- Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI.
- Métricas de desempeño de los procesos (indica si es probable alcanzar las metas).

La relación entre las metas de negocio de TI, de proceso y de las actividades, y las diferentes métricas. (Figura A.6)

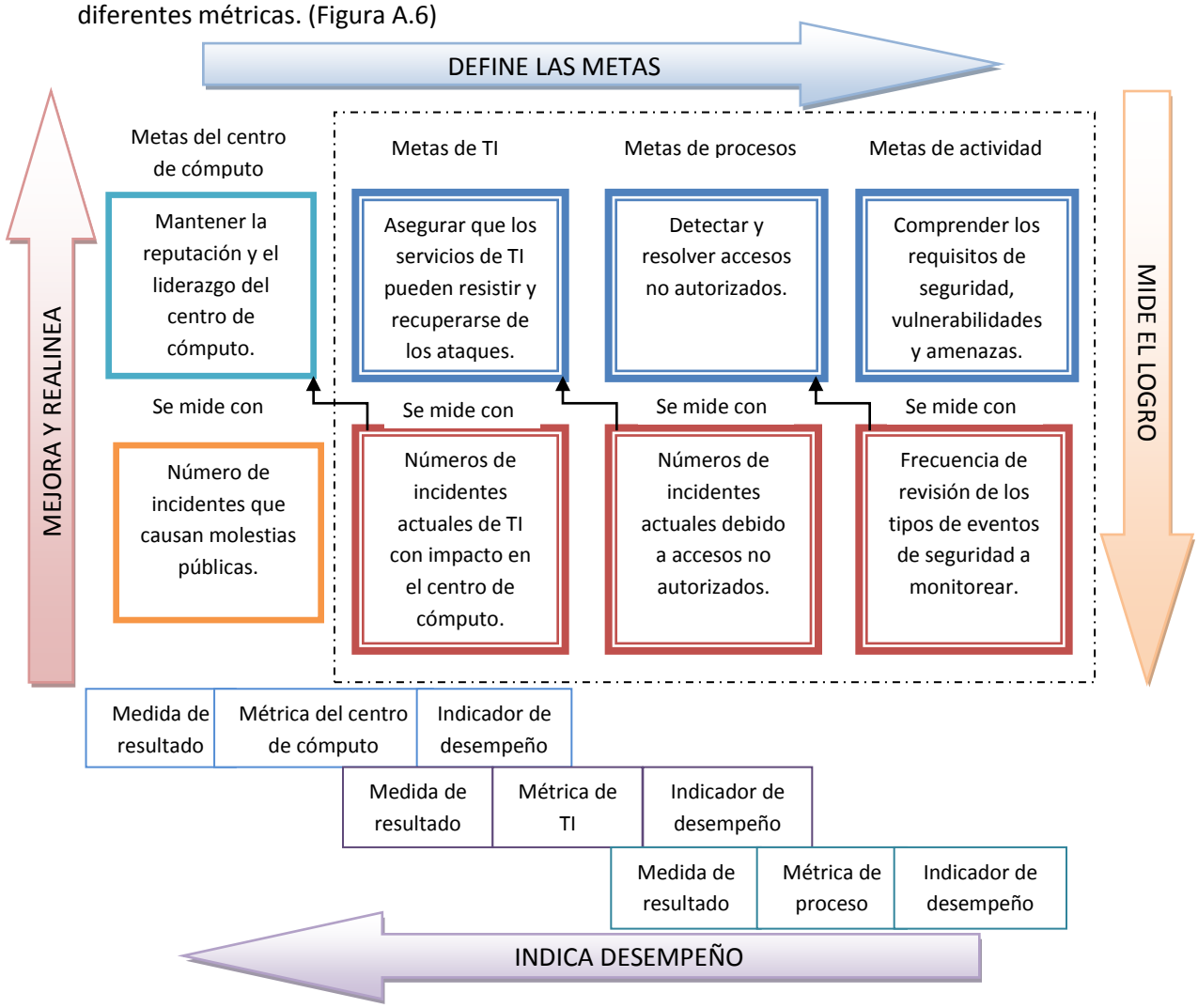

Figura A.6 Relación entre procesos, metas y métricas (DS5)

MODELO DEL MARCO DE TRABAJO DE COBIT

El marco de trabajo COBIT, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicios de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las metas y métricas de COBIT, como se ilustra en la figura A.7.

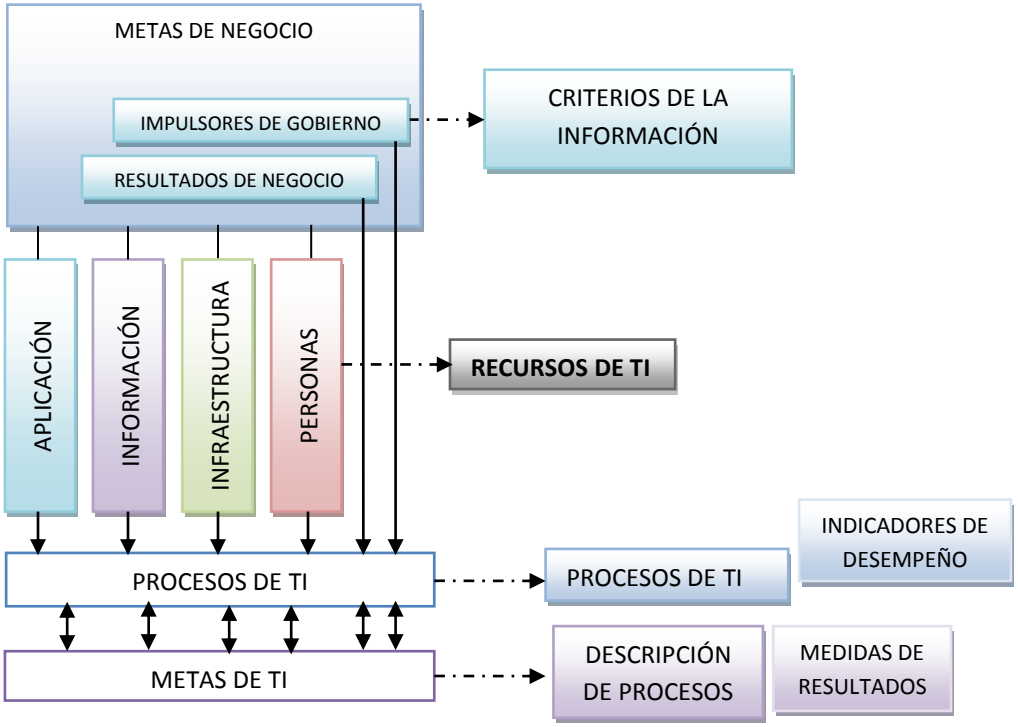

Figura A.7 COBIT Gestión, control, alineamiento y monitoreo

Los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Éste es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT (Figura A.8)

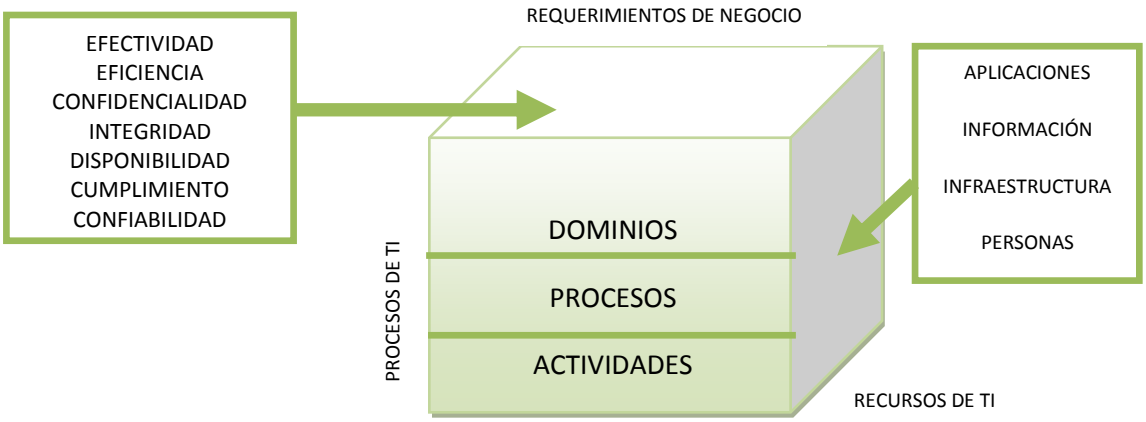

Figura A.8 El cubo de COBIT

El marco de trabajo general COBIT se muestra gráficamente (Figura A.9), con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

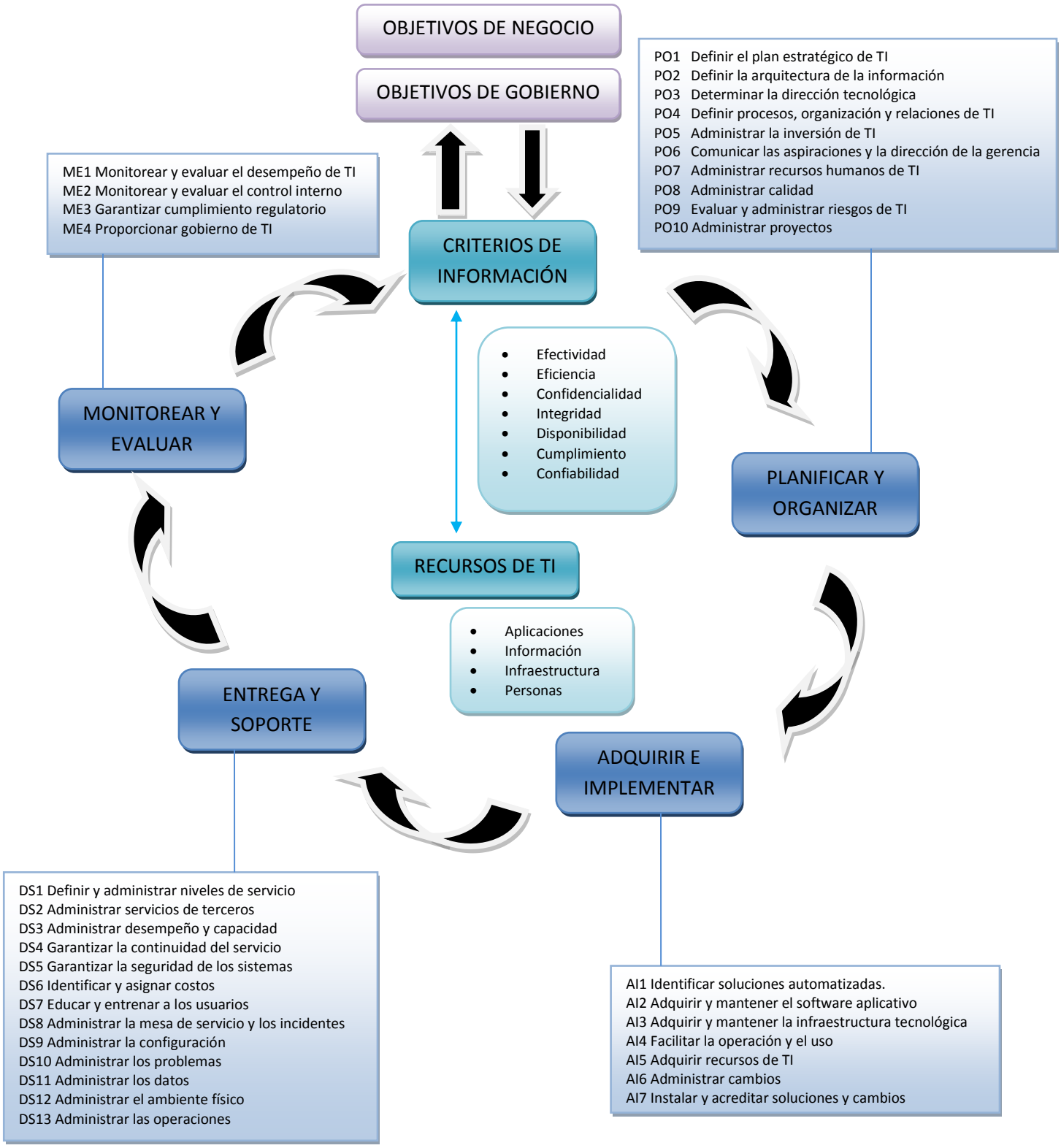

Figura A.9 Marco de trabajo de COBIT

PLANEAR Y ORGANIZAR

PO1 Definir el plan estratégico de TI

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.

El plan estratégico satisface el requerimiento del negocio de TI para sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos.

Se logra con:

- El compromiso con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras.
- El entendimiento de las capacidades actuales de TI.
- La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio.

Etapas para definir un correcto plan estratégico de TI:

1) Administración del Valor de TI

   Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

2) Alineación de TI con el Negocio

   Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

3) Evaluación del Desempeño y la Capacidad Actual

   Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

4) Plan Estratégico de TI

Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados.

5) Planes Tácticos de TI

Los planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios.

6) Administración del Portafolio de TI

Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.

PO2 Definir la arquitectura de la información

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones asegurando que se proporciona información confiable y segura.

Satisface el requerimiento del negocio de TI para agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio. Enfocándose en el establecimiento de un modelo de datos que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.

Se logra con:

- El aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos.
- La asignación de propiedad de datos.
- La clasificación de la información usando un esquema de clasificación acordado.

PO3 Determinar la dirección tecnológica

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas claras de lo que la tecnología puede ofrecer en términos de productos, servicio y mecanismos de aplicación. El plan se debe actualizar de forma regular, abarca aspectos como arquitectura de sistemas, dirección tecnológica, planes de

adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo.
La dirección tecnológica se enfoca en la definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.

Se logra con:

- El establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento.
- El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos.
- La definición de estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información.

Para determinar la dirección tecnológica se debe:

- Analizar las tecnologías existentes para planear la dirección tecnológica.
- Crear un plan de infraestructura tecnológica.
- Monitorear las tendencias y regulaciones futuras.
- Conocer los estándares tecnológicos.
- Establecer un consejo de arquitectura de TI.

PO4 Definir procesos, organización y relaciones de TI

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión.

Se enfoca en el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión.

Se logra con:

- La definición de un marco de trabajo de procesos de TI.
- El establecimiento de un cuerpo y una estructura organizacional apropiada.
- La definición de roles y responsabilidades.

Para definir los procesos, organización y relaciones de TI se tiene que:

- Definir un marco de trabajo de procesos de TI.
- Establecer un comité estratégico de TI.
- Establecer un comité directivo de TI.
- Ubicar la organización de la función de TI.
- Establecer una estructura organizacional.
- Establecer los roles y responsabilidades para el personal de TI.
- Asignar responsabilidades para el aseguramiento de la calidad de TI.
- Establecer responsabilidades sobre el riesgo, la seguridad y el cumplimiento.
- Propiedad de datos y de sistemas.

- Implementar la supervisión.
- Segregar funciones.
- Evaluar al personal de TI.
- Identificar al personal clave de TI.
- Asegurar el cumplimiento de políticas y procedimientos para el personal contratado.
- Establecer y mantener relaciones de comunicación y coordinación entre la función de TI.

PO5 Administrar la inversión de TI

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios y prioridades dentro del presupuesto.

Con esto se mejora la rentabilidad de TI y su contribución que satisfaga las expectativas del usuario. Se enfoca en decisiones de inversión de TI de manera efectiva, eficiente, el establecimiento y seguimiento de presupuestos de TI, de acuerdo a la estrategia de TI y a las decisiones de inversión.

Se logra con:

- El pronóstico y la asignación de presupuestos.
- La definición de criterios formales de inversión.
- La medición y evaluación del valor del negocio en comparación con el pronóstico.

Para administrar la inversión se requiere:

- Establecer un marco de trabajo para la administración financiera.
- Implementar un proceso para conocer las prioridades dentro del presupuesto de TI.
- Establecer un proceso presupuestal.
- Administrar los costos de TI.
- Administrar los beneficios.

PO6 Comunicar las aspiraciones y la dirección de la gerencia

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas.

Esto satisface una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades. Enfocándose en proporcionar políticas, procedimientos, directrices y documentación de forma precisa y entendible.

Se logra con:

- La definición de un marco de trabajo de control para TI.
- La elaboración e implementación de políticas para TI.
- El esfuerzo de políticas de TI.

Para comunicar las aspiraciones se requiere:

- Definir un ambiente de políticas y de control.
- Elaborar la administración de políticas de TI.

- Implementar las políticas de TI.
- Asegurarse que haya comunicación de los objetivos y la dirección de TI.

PO7 Administrar recursos humanos de TI

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Con esto se pretende adquirir gente competente y motivada para crear y entregar servicios de TI. Enfocándose en la contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de puestos y el aseguramiento de la dependencia sobre los individuos.

Se logra con:

- La revisión del desempeño personal.
- La contratación y entrenamiento de personal de TI para apoyar los planes técnicos de TI.
- La mitigación del riesgo de sobre-dependencia de recursos clave.

Para llevar a cabo la administración de recursos humanos de TI se requiere

- Reclutar y retener al personal que esté de acuerdo con las políticas.
- Realizar competencias del personal.
- Asignar roles.
- Entrenar al personal de TI.
- Minimizar la exposición a dependencias sobre los individuos.
- Realizar procedimientos de investigación del personal.
- Evaluar el desempeño del empleado.
- Tomar medidas respecto a cambios y terminación de trabajo.

PO8 Administrar calidad

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos, estándares de desarrollo y de adquisición. Esto satisface la mejora continua y medible de los servicios prestados por TI.

Se logra con:

- La definición de estándares y prácticas de calidad.
- El monitoreo y revisión interna del desempeño contra estándares y prácticas de calidad definidas.

Para llevar una correcta administración de la calidad de debe:

- Establecer un sistema de administración de calidad.
- Identificar estándares y prácticas de calidad.
- Adoptar estándares de desarrollo y de adquisición.
- Enfocar la administración de calidad en los clientes de TI.
- Mantener un plan de calidad que promueva la mejora continua.
- Medir, monitorear y revisar la calidad.

PO9 Evaluar y administrar riesgos de TI

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. Esto satisface el requerimiento del negocio al analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio.

Se logra con:

- La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interno y externo, se aplica de forma consistente.
- La realización de evaluaciones de riesgo.
- La recomendación y comunicación de planes para remediar riesgos.

Para evaluar y administrar los riesgos de TI se debe:

- Establecer un marco de trabajo de administración de riesgos.
- Establecer el contexto del riesgo.
- Identificar eventos.
- Evaluar los riesgos de TI.
- Desarrollar y mantener un proceso de respuesta a los riesgos.
- Mantener y monitorear un plan de acción de riesgos.

PO10 Administrar proyectos

Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. Se satisface este requerimiento para la entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados.

Se logra con:

- La definición e implantación de marcos de trabajo y enfoques de programas y de proyectos.
- La planeación de proyectos.

Para administrar los proyectos se debe:

- Establecer un marco de trabajo para la administración de proyectos.
- Establecer un enfoque de administración de proyectos.
- Obtener el compromiso de los interesados.
- Definir y documentar el alcance del proyecto.
- Aprobar el inicio de las fases del proyecto.
- Definir las responsabilidades y los recursos del proyecto.
- Administrar los riesgos del proyecto.
- Preparar un plan de calidad del proyecto.
- Establecer un control de cambios del proyecto.
- Medir el desempeño, reportar y monitorear el proyecto.
- Finalizar el proyecto, asegurándose de proporcionar los resultados esperados.

ADQUIRIR E IMPLEMENTAR

AI1 Identificar soluciones automatizadas.

Satisface el requerimiento del negocio de TI para traducir los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas, enfocándose en la identificación de soluciones factibles y rentables.

Se logra con:

- La definición de los requerimientos técnicos y de negocio.
- Realizar estudios de factibilidad como se definen en los estándares de desarrollo.
- Aprobar o rechazar los requerimientos y los resultados de los estudios de factibilidad.

Para identificar las soluciones automatizadas se debe

- Definir y dar mantenimiento de los requerimientos técnicos y funcionales del negocio.
- Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio.
- Desarrollar un estudio de factibilidad y formulación de cursos de acción.
- Revisar si se cumplieron los requerimientos, la decisión de factibilidad y aprobarlos.

AI2 Adquirir y mantener el software aplicativo

Se deben construir las aplicaciones de acuerdo con los requerimientos del negocio, enfocándose en garantizar que exista un proceso de desarrollo oportuno y confiable.

Se logra con:

- La traducción de requerimientos de negocio a especificaciones de diseño.
- La adopción de estándares de desarrollo para todas las modificaciones.
- La separación de las actividades de desarrollo, de pruebas y operativas.

Para adquirir y mantener el software aplicativo se debe:

- Traducir los requerimientos del negocio a un diseño de alto nivel.
- Prepara el diseño detallado.
- Implementar el control y la posibilidad de auditar las aplicaciones.
- Abordar la seguridad y disponibilidad de las aplicaciones.
- Configurar e implementar software de aplicaciones adquiridas.
- Actualizar los sistemas.
- Garantizar la funcionalidad del desarrollo de software aplicativo.
- Desarrollar, implementarlos recursos y ejecutar un plan de aseguramiento de la calidad del software.
- Administrar los requerimientos de aplicaciones.
- Desarrollar un plan de mantenimiento de aplicación de software.

AI3 Adquirir y mantener la infraestructura tecnológica

Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto se requiere para adquirir y dar mantenimiento a un

infraestructura integrada y estándar de TI. Enfocándose en proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

Se logra con:

- El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica.
- La planeación de mantenimiento de la infraestructura.
- La implantación de medidas de control interno, seguridad y auditabilidad.

Al adquirir y mantener la infraestructura tecnológica se debe

- Generar un plan de adquisición de infraestructura tecnológica.
- Implementar la protección y disponibilidad del recurso de infraestructura.
- Desarrollar un plan de mantenimiento de la infraestructura.
- Establecer un ambiente de prueba de factibilidad.

AI4 Facilitar la operación y el uso

El conocimiento sobre los nuevos sistemas debe estar disponible. Enfocándose en proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitoso del sistema.

Se logra con:

- El desarrollo y la disponibilidad de documentación para trasferir el conocimiento.
- Comunicación y entrenamiento a usuarios y a la gerencia del negocio, al personal de apoyo al personal de operación.
- La generación de materiales de entrenamiento.

Al facilitar la operación y el uso se debe:

- Desarrollar un plan para soluciones de operación.
- Trasferir el conocimiento a la gerencia del negocio.
- Trasferir el conocimiento a usuarios finales.
- Transferir el conocimiento al personal de operaciones y soporte.

AI5 Adquirir recursos de TI

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Enfocándose en adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI.

Se logra con:

- La obtención de asesoría profesional legal.
- La definición de procedimientos y estándares de adquisición.
- La adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos.

Al adquirir recursos de TI se debe:

- Desarrollar un control de adquisición.
- Formular un procedimiento para la administración de contratos con proveedores.
- Seleccionar los proveedores.
- Proteger y hacer cumplir los intereses de la organización al adquirir recursos de TI.
- Administrar cambios.
- Instalar y acreditar soluciones y cambios.

AI6 Administrar cambios

Todos los cambios deben administrarse formalmente y controladamente. Enfocándose en controlar la evaluación del impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, tratando de minimizar errores.

Se logra con:

- La definición y comunicación de los procedimientos de cambio, que incluyen cambios de emergencia.
- La evaluación, la asignación de prioridad y autorización de cambios.
- Seguimiento del estatus y reporte de los cambios.

Al administrar los cambios se debe:

- Establecer procedimientos y estándares para cambios.
- Priorizar, autorizar y evaluar el impacto.
- Establecer cambios de emergencia.
- Establecer el seguimiento y reportar el estatus del cambio.
- Documentar el cambio al finalizar el análisis.

AI7 Instalar y acreditar soluciones y cambios

Contar con sistemas nuevos o modificados que trabajan sin problemas después de la instalación. Enfocándose en probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y están libres de errores, y planear las liberaciones a producción.

Se logra con:

- El establecimiento de una metodología de prueba.
- Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio.
- Ejecutar revisiones posteriores a la implantación.

Al instalar y acreditar soluciones y cambios se debe:

- Entrenar al personal de los departamentos de usuario afectados.
- Establecer un plan de prueba.
- Establecer un plan de implantación.
- Definir y establecer un ambiente de prueba.
- Establecer un plan de conversión de sistemas y datos.
- Realizar pruebas de cambios.
- Asegurar las pruebas de aceptación final.
- Darle un seguimiento a las pruebas.

- Establecer procedimientos para la revisión posterior a la implantación.

ENTREGAR Y DAR SOPORTE

DS1 Definir y administrar niveles de servicio

Asegura la alineación de los servicios claves de TI con la estrategia del negocio. Enfocándose en la identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.

Se logra con:

- La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades entrega La notificación del cumplimiento de los niveles de servicio (reportes y reuniones).
- La identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica.

Al definir y administrar niveles de servicio se debe:

- Definir un marco de trabajo de la administración de los niveles del servicio.
- Definir los servicios.
- Acordar los niveles de servicio.
- Asegurar los acuerdos de niveles de operación.
- Monitorear y reportar el cumplimiento de los niveles de servicio.
- Revisar los acuerdos de niveles de servicio y de los contratos.

DS2 Administrar servicios de terceros

Se pretende brindar servicios satisfactorios a terceros con transparencia acerca de los beneficios, riesgos y costos. Enfocándose en el establecimiento de relaciones y responsabilidades con proveedores calificados de los servicios, verificando y asegurando los convenios.

Y se logra con:

- La identificación y categorización de los servicios del proveedor.
- La identificación y mitigación de riesgos del proveedor.
- El monitoreo y la medición del desempeño del proveedor.

Al administrar servicios de terceros se debe:

- Identificar todas las relaciones con los proveedores.
- Formalizar la gestión de relaciones con los proveedores.
- Administrar los riesgos del proveedor.
- Monitorear el desempeño del proveedor.

DS3 Administrar el desempeño y la capacidad

Esto requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Con el propósito de optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio. Enfocándose en cumplir con los requerimientos de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin

servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición

Se logra con:

- La planeación y la entrega de capacidad y disponibilidad del sistema.
- Monitoreando y reportando el desempeño del sistema.
- Modelando y pronosticando el desempeño del sistema.

Al administrar el desempeño y la capacidad se debe:

- Establecer un proceso de planeación del desempeño y la capacidad.
- Revisar la capacidad y el desempeño actual.
- Llevar a cabo un pronóstico de capacidad y desempeño futuros.
- Disponer de los recursos de TI.
- Monitorear continuamente y realizar un reporte.

DS4 Garantizar la continuidad del servicio

Satisface el requerimiento del negocio de TI para asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI. Enfocándose en el desarrollo de resistencia en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.

Se logra con:

- Desarrollando y manteniendo (mejorando) los planes de contingencia de TI.
- Con entrenamiento y pruebas de los planes de contingencia de TI.
- Guardando copias de los planes de contingencia y de los datos fuera de las instalaciones.

Al garantizar la continuidad del servicio se debe:

- Desarrollar un marco de trabajo de continuidad de TI.
- Desarrollar planes de continuidad de TI.
- Determinar los recursos críticos de TI.
- Realizar mantenimiento del plan de continuidad de TI.
- Realizar pruebas de continuidad de TI.
- Preparación del plan de continuidad de TI.
- Distribuir el plan de continuidad de TI.
- Recuperar y reanudar los servicios de TI.
- Almacenar respaldos fuera de las Instalaciones.
- Realizar una revisión después de la reanudación.

DS5 Garantizar la seguridad de los sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. Monitorear, detectar, reportar y dar solución a las vulnerabilidades e incidentes de seguridad.

Se logra con:

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular.

Al garantizar la seguridad de los sistemas se debe:

- Administrar la seguridad de TI.
- Establecer un plan de seguridad de TI.
- Administración de Identidad.
- Administrar cuentas del usuario.
- Realizar pruebas y monitorear la seguridad.
- Definir si hay incidentes de seguridad.
- Proteger la tecnología de seguridad.
- Administrar claves criptográficas.
- Prevenir, detectar y corregir software malicioso.
- Administrar la seguridad de la red.

DS6 Identificar y asignar costos

Mejora la rentabilidad a través del uso bien informado de los servicios de TI. Realizando un registro completo y preciso de los costos de TI, un sistema equitativo para la asignación acordado con los usuarios. Es necesario un sistema para reportar oportunamente el uso de TI y los costos asignados.

Se logra con:

- La alineación de cargos con calidad y cantidad de los servicios brindados.
- La construcción y aceptación de un modelo de costos completo.
- La aplicación de cargos con base en la política acordada.

Al identificar y asignar costos se debe:

- Definir los servicios.
- Contabilización de TI.
- Modelar los costos y cargos.
- Llevar a cabo el mantenimiento del modelo de costos.

DS7 Educar y entrenar a los usuarios

Se enfoca en un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.

Se logra con:

- Establecer un programa de entrenamiento.
- Organizar el entrenamiento.
- Impartir el entrenamiento.
- Monitorear y reportar la efectividad del entrenamiento.

Al educar y entrenar a los usuarios se debe:

- Identificar las necesidades de entrenamiento y educación.
- Impartir el entrenamiento y la educación.
- Evaluar el entrenamiento recibido.

DS8 Administrar la mesa de servicio y los incidentes

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Se enfoca en una función profesional, con el tiempo de respuesta rápido, procedimientos de escalamiento claros y análisis de tendencias y de resolución.

Se logra con:

- Instalación y operación de un servicio de una mesa de servicios.
- Monitoreo y reporte de tendencias.
- Definición de procedimientos y de criterios de escalamiento claros.

Al administrar la mesa de servicio y los incidentes se debe:

- Establecer la función de mesa de servicio.
- Registrar las consultas de los clientes.
- Establecer procedimientos para el escalamiento de incidentes.
- Establecer procedimientos para el monitoreo y la resolución de incidentes.
- Analizar las tendencias.

DS9 Administrar la configuración

Garantizar la integridad de las configuraciones de hardware y software. Enfocándose en establecer y mantener un reporte completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

Se logra con:

- El establecimiento de un reporte central de todos los elementos de la configuración.
- La identificación de los elementos de configuración y su mantenimiento.
- Revisión de la integridad de los datos de configuración.

Al administrar la configuración se debe:

- Realizar un reporte y línea base de configuración.
- Identificar, dar un mantenimiento a los elementos de configuración.
- Revisar la integridad de la configuración.

DS10 Administrar los problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. Enfocándose a registrar, rastrear y resolver problemas operativos.

Se logra con:

- Realizando un análisis de causas raíz de los problemas reportados.
- Analizando las tendencias.
- Tomando propiedad de los problemas y con una resolución de problemas progresiva.

Al administrar los problemas se debe:

- Implementar procesos para identificar, clasificar y reportar los problemas.
- Rastrear y resolver los problemas.
- Cerrar los registros de problemas.
- Integrar la administración de cambios, configuración y problemas.

DS11 Administrar los datos

El proceso de administración de información incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Este proceso optimiza el uso de la información y garantiza la disponibilidad de la información cuando se requiera. Enfocándose en mantener la integridad, exactitud, disponibilidad y protección de los datos.

Se logra con:

- Respaldando los datos y probando la restauración.
- Administrando el almacenamiento de datos en el sitio y fuera del sitio.
- Desechando de manera segura los datos y el equipo.

En la administración de datos se debe:

- Verificar que todos los datos que se espera procesar se reciban. Los requerimientos del negocio para la administración de datos.
- Definir acuerdos de almacenamiento y conservación.
- Definir e implementar un sistema de administración de librerías de medios.
- Definir e implementar procedimientos para asegurar la trasferencia o la eliminación de datos.
- Realizar un respaldo y restauración de los sistemas.
- Definir e implementar los requerimientos de seguridad para la administración de datos.

DS12 Administrar el ambiente físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El objetivo es proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio. Para proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo

Se logra con:

- Implementando medidas de seguridad físicas.
- Seleccionando y administrando las instalaciones.

En la administración del ambiente físico se debe:

- Definir, seleccionar y diseñar el centro de datos.

- Definir e implementar medidas de seguridad física.
- Definir e implementar procedimientos para otorgar, limitar y revocar el acceso físico.
- Definir e implementar medidas de protección contra factores ambientales.
- Administrar las instalaciones físicas.

DS13 Administrar las operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida, monitores de infraestructura y mantenimiento preventivo de hardware.

Se logra con:

- Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas.
- Manteniendo la infraestructura de TI.

Al administrar las operaciones se debe:

- Definir e implementar procedimientos e instrucciones de operación.
- Organizar la programación de tareas.
- Definir e implementar procedimientos para monitorear la infraestructura de TI.
- Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos.
- Definir e implementar procedimientos de mantenimiento preventivo del hardware.

MONITOREAR Y EVALUAR

ME1 Monitorear y evaluar el desempeño de TI

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. Este proceso se requiere para tener una transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno. Enfocándose en monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño.

Se logra con:

- Cotejar y traducir los reportes de desempeño de proceso a reportes gerenciales.
- Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias.

Al monitorear y evaluar el desempeño de TI se debe:

- Establecer un enfoque del monitoreo.
- Definir y recolectar datos de monitoreo.
- Garantizar el método de monitoreo.

- Evaluar el desempeño.
- Reportar a los directivos y ejecutivos.
- Realizar acciones correctivas.

ME2 Monitorear y evaluar el control interno

Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

Se logra con:

- La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI.
- Monitorear y reportar la efectividad de los controles internos sobre TI.
- Reportar las excepciones de control a la gerencia para tomar decisiones.

Al monitorear y evaluar el control interno se debe:

- Monitorear de forma continua, comparar y mejorar el ambiente de control de TI.
- Monitorear y evaluar la eficiencia y la efectividad realizando revisiones de auditoría.
- Identificar las excepciones de control.
- Evaluar la efectividad de los controles llevando a cabo una auto evaluación.
- Asegurar el control interno.
- Evaluar el estado de los controles internos de los proveedores de servicios externos.
- Identificar, iniciar, rastrear e implementar acciones correctivas.

ME3 Garantizar el cumplimiento regulatorio

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos. Enfocándose en la identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.

Se logra con:

- La identificación de los requisitos legales y regulatorios relacionados con TI.
- La evaluación del impacto de los requisitos regulatorios.
- El monitoreo y reporte del cumplimento de los requisitos regulatorios.

Al garantizar el cumplimiento regulatorio se debe:

- Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales.
- Optimizar la respuesta a requerimientos externos.
- Evaluar el cumplimiento con los requerimientos externos.
- Asegurar el cumplimiento de las políticas internas o requerimientos legales.
- Integrar reportes de TI sobre los requerimientos legales.

ME4 Proporcionar gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades. Enfocándose en la elaboración de informes para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI.

Se logra con:

- El establecimiento de un marco de trabajo para el gobierno de TI, integrado al gobierno corporativo.
- La obtención de aseguramiento independiente sobre el estatus del gobierno de TI.

Al proporcionar gobierno de TI se debe:

- Definir, establecer y alinear el marco de gobierno de TI.
- Llevar a cabo el alineamiento estratégico.
- Administrar los programas de inversión habilitados por TI.
- Administrar los recursos.
- Administrar los riesgos.
- Medir el desempeño.
- Garantizar de forma independiente (interna o externa) la conformidad de TI con la legislación y regulación relevante.

REFERENCIAS

Trabajos citados

ADN. (2013). Obtenido de http://ciencia.glosario.net/genetica/adn-dna-4813.html

Altos ejecutivos. (2013). Obtenido de http://www.uia.mx/actividades/publicaciones/iberoforum/2/pdf/marisol_joseluis.pdf

Análisis FODA. (2013). Obtenido de http://www.cca.org.mx/funcionarios/cursos/ap089/apoyos/m3/analisis.pdf

Antimalware. (2013). Obtenido de http://es.wikipedia.org/wiki/Malware

Antispyware. (2013). Obtenido de http://www.alegsa.com.ar/Diccionario/C/9296.php

Buenas prácticas. (2013). Obtenido de http://www.fao.org/knowledge/goodpractices/good-practice-cycle/es/

Buenas prácticas, estándares y normas. (2013). Obtenido de http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

Ciberbullyng. (2013). Obtenido de http://es.wikipedia.org/wiki/Ciberacoso

Cifrado AES. (2013). Obtenido de http://es.wikipedia.org/wiki/Advanced_Encryption_Standard#Seguridad

Cifrado DES. (2013). Obtenido de http://es.wikipedia.org/wiki/Triple_DES#Usos

Círculo de Deming. (2013). Obtenido de http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

COBIT. (2013). Obtenido de http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

COBIT. (2013). Obtenido de http://mba.americaeconomia.com/sites/mba.americaeconomia.com/files/cobit5-introduccion.pdf

Comunicación alámbrica. (2013). Obtenido de http://tecnocomunicaciones.wikispaces.com/COMUNICACI%C3%93N+AL%C3%81MBRICA

Concepto de amenaza. (2013). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

Concepto de vulnerabilidad. (2013). Obtenido de http://www.slideshare.net/Tcherino/seguridad-informatica-3143924

Daltabuit Godás, E., Hernández Audelo, L., Mallén Fullerton, G., & Vázquez Gómez, J. d. (2007). La seguridad de la información. México: Limusa.

Definición de administración. (2013). Obtenido de http://www.elprisma.com/apuntes/administracion_de_empresas/conceptodeadministracion/

Definición de información. (2013). Obtenido de http://www.eduteka.org/modulos/1/3/

Definición de organización. (2013). Obtenido de http://www.elprisma.com/apuntes/administracion_de_empresas/organizacion/

Desarrollador de software. (2013). Obtenido de http://es.wikipedia.org/wiki/Desarrollador_de_software

Dispositivos inalámbricos. (2013). Obtenido de http://www.slideshare.net/AnnieJuliana/dispositivos-inalmbricos

Herramientas de monitoreo de red. (2013). Obtenido de http://insecure.org/tools/tools-es.html

Libro de administración básica. UNAM ABIERTA. (2003). Obtenido de http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/1/admon_bas1.pdf

Libro de admnistración básica. UNAM ABIERTA. (2011). Obtenido de http://fcasua.contad.unam.mx/apuntes/interiores/docs/2011/contaduria/1/admon_basica.pdf

López Barrientos, M. J., & Quezada Reyes, C. (2006). En *Fundamentos de seguridad informática.* (pág. 223). México: UNAM, Facultad de Ingeniería.

Monitoreo de red. (2013). Obtenido de http://es.wikipedia.org/wiki/Monitoreo_de_red

Monitoreo de red. (2013). Obtenido de http://insecure.org/tools/tools-es.html

Olguín, H. (2013). *Organización y administración de centros de cómputo. Versión dígital.* Obtenido de http://profesores.fi-b.unam.mx/heriolg/portada.pdf

Plan de contingencias. (2013). Obtenido de http://www.segu-info.com.ar/politicas/contingencia.htm

Plan de contingencias. (2013). Obtenido de http://www.seguridad-la.com/artic/segcorp/7209.htm

Plan de contingencias. (2013). Obtenido de http://www.cne.go.cr/CEDO-CRID/pdf/spa/doc1071/doc1071-c.pdf

Políticas de seguridad. (2013). Obtenido de http://www.monografias.com/trabajos11/seguin/seguin.shtml#meto

Políticas de seguridad. (2013). Obtenido de http://auditoriasistemas.com/auditoria-informatica/politicas-de-seguridad/

Protección de datos en Internet. (2013). Obtenido de http://www.zocalo.com.mx/seccion/articulo/tips-para-proteger-tus-datos-en-internet

Quezada Reyes, C. (2008). Apuntes de seguridad informática I.

Red ad hoc. (2013). Obtenido de http://es.wikipedia.org/wiki/Red_ad_hoc

Redes inalámbricas. (2013). Obtenido de http://es.kioskea.net/contents/wireless/wlintro.php3

Sandoval Vázquez, R. (2009). Apuntes de seguridad informática II.

Seguridad de la información. (2013). Obtenido de http://www.segu-info.com.ar/

Seguridad de la red. (2013). Obtenido de http://fmc.axarnet.es/REDES/tema_10_m.htm

Seguridad de la red. (2013). Obtenido de http://www.wlana.org/learn/educate.htm

Seguridad de la red. (2013). Obtenido de http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

Seguridad de la red. (2013). Obtenido de http://alerta-antivirus.red.es/portada/

Sistema de gestión de calidad. (2013). Obtenido de http://seicoboletin.blogspot.mx/2011/05/sistemas-de-gestion-de-calidad.html

Tecnologías de Internet. (2013). Obtenido de http://es.wikibooks.org/wiki/Tecnolog%C3%ADas_de_Internet/La_Internet

Tecnologías de Internet. (2013). Obtenido de HTTP://ES.WIKIBOOKS.ORG/WIKI/TECNOLOG%C3%ADAS_DE_INTERNET/LA_WEB

TIC´S. (2013). Obtenido de http://www.slideshare.net/DAFRAGA/tics-caractersticas-clasificacin

TIC'S. (2013). Obtenido de http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html

TIC'S. (2013). Obtenido de http://www.serviciostic.com/las-tic/definicion-de-tic.html

TIC'S. (2013). Obtenido de http://www.tics.org.ar/home/index.php/noticias-destacadas-2/157-definicion-de-tics

TIC'S. (2013). Obtenido de http://www.slideshare.net/bibianapaola/ventajas-y-desventajas-de-las-tics-6884061

TIC'S en los procesos de enseñanza y aprendizaje. (2013). Obtenido de http://educatics.blogspot.mx/

TIC'S enn la informática. (2013). Obtenido de http://es.scribd.com/doc/3285023/TICS-EN-LA-INFORMATICA

VPN. (2013). Obtenido de http://es.kioskea.net/contents/initiation/vpn.php3

WAP. (2013). Obtenido de http://es.wikipedia.org/wiki/Wireless_Application_Protocol

WEP. (2013). Obtenido de http://es.wikipedia.org/wiki/Wired_Equivalent_Privacy

WIFI. (2013). Obtenido de http://www.aulaclic.es/articulos/wifi.html

WIFI. (2013). Obtenido de http://definicion.de/wifi/

WIFI. (2013). Obtenido de http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access

WIMAX. (2013). Obtenido de http://es.wikipedia.org/wiki/WiMAX

WPAN. (2013). Obtenido de http://es.kioskea.net/contents/wireless/wpan.php3

Zona desmilitarizada. (2013). Obtenido de http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)