UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ADMINISTRACIÓN DE LA SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A

DULCE CAMPOS DEL RAZO

DIRECTOR DE TESIS:

ING. RAFAEL SANDOVAL VÁZQUEZ

México, D.F. 2008

Ciudad Universitaria

DEDICATORIA

Primeramente se la dedico a DIOS quien nos da la bendición de despertar y tener un nuevo día, sin Él no somos nada.

También se la dedico a mi madre Teresa del Razo Alvarado, gracias por tu amor, tu apoyo, tu bendición y por todas las oraciones que haces por mí, Dios siempre te escucha.

Por último se la dedico con un gran cariño y amor a la memoria de mi padre el Ing. Fernando Campos Ibarra con quién construí el sueño de ser Ingeniera. Siempre te tengo en mis más bonitos recuerdos, nunca olvidaré tus enseñanzas, siempre fuiste el pilar de la familia.

Dulce Campos del Razo.

AGRADECIMIENTOS

Es difícil agradecer a todos deseando no olvidar ningún nombre, pero sé muy bien que la gente que quiero y que ha sido importante en mi vida, sabe el gran cariño y agradecimiento que les tengo por estar conmigo en las buenas y en las malas.

Sin embargo no puedo dejar de agradecer a mi familia; a mis papás (Tere y Fer), mis hermanos (Hugo y Cinthia), mis sobrinos (Monse, Josy y Pablito) y mis tías (Rosy y Maru). A la Universidad Nacional Autónoma de México (UNAM), bella universidad de la cual estoy orgullosa de pertenecer, se que fui una afortunada entre tantos jóvenes. A la Facultad de Ingeniería por ser mi segunda casa y por haberme permitido ser parte de su comunidad, como olvidar esos días en que llegaba de madrugada y me iba de noche. A UNICA por permitirme ser parte del programa de becarios, sin duda muchas cosas que aprendí en la unidad fueron muy valiosas para mi formación académica. Al Departamento de Seguridad en Cómputo en especial al Ing. Rafael Sandoval Vázquez por permitirme la realización de esta tesis en el departamento y sus consejos para la elaboración. A todos los becarios y jefes por darme su apoyo en uno de los momentos más difíciles de mi vida. Y lo prometido es deuda, agradezco a todos aquellos que pusieron un granito en mi tesis y que prometí ponerlos en mis agradecimientos.

No temas, que yo soy contigo;
no desmayes, que yo soy tu Dios
que te esfuerzo;
siempre te ayudaré,
siempre te sustentaré
con la diestra de mi justicia
Isaías 41:10

Administración de la Seguridad en Tecnologías de la Información

Prólogo

Las tendencias en el mundo como la globalización, avance tecnológico y la competencia llevan a las organizaciones a redefinir sus estrategias para alcanzar sus objetivos. Por lo que requieren de una mayor intervención de las Tecnologías de la Información (TI), obligándolas a estar a la vanguardia en sus sistemas de información.

Sin duda, la necesidad de las TI se ha convertido en una realidad. Las TI llegan a ser una herramienta poderosa para ayudar a definir las estrategias, optimizar la organización y manejo de la información y así incrementar la productividad.

Los servicios TI dejaron de ser funciones meramente operativas y de soporte, para integrarse a la arquitectura organizativa aportando valor al negocio y servicios.

El diseño de las organizaciones TI se enfoca desde un cambio de paradigma, al abandonar la visión centrada en sus productos. Desarrollan su filosofía entorno a una organización basada en procesos. Para esto es necesario poner su visión en algún estándar que lo ayude a tener una mayor fiabilidad y efectividad de sus activos.

La estandarización a nivel internacional juega un papel importante en el sector industrial, fabricantes, distribuidores y el usuario final. Facilitan enormemente a la organización en cuanto al manejo de sus procesos y controles ayudándole a crecer día a día.

Existen estándares como el Modelo de Madurez de Gestión de la Seguridad de la Información (ISM3), que se enfoca en la "seguridad alcanzable", en lugar de la "seguridad absoluta". La seguridad alcanzable es un equilibrio entre la seguridad absoluta y los requerimientos de negocio y de servicios. La clásica percepción de que la "seguridad de la información debe prevenir todos los ataques", no es realista para muchas de las organizaciones. ISM3 alcanza su balance mediante el mapeo de los objetivos de negocio y servicio (como cadena de producción y rentabilidad, accesibilidad, disponibilidad entre otros) directamente contra los objetivos de seguridad (como asegurar el acceso a los datos sólo para usuarios autorizados).

Introducción

Este trabajo de tesis permitió seleccionar el estándar o modelo de gestión de procesos más adecuado para él funcionamiento de las actividades cotidianas del Departamento de Seguridad en Cómputo de la Facultad de Ingeniería.

El primer capítulo nos da una pequeña introducción sobre la seguridad informática, explicando conceptos básicos de la misma, los cuáles nos clarifican y nos forman un marco de referencia. También nos habla sobre los objetivos de seguridad informática, los servicios, las amenazas y la cultura de seguridad que existe o debiera existir en una organización.

El capítulo dos nos ayudará a comprender los requisitos que necesita una organización para tener una adecuada gestión de la seguridad, explicando a detalle los procesos que se deben realizar para la administración de las tecnologías de la información. Cabe señalar que este capítulo nos ayuda a comprender la importancia de la seguridad en las TI y la forma en que se puede implementar en la organización viéndola como una herramienta importante para su crecimiento.

El tercer capítulo explica los modelos de seguridad existentes. Se definen las Normas y Regulaciones tanto Internacionales como Nacionales que requieren las organizaciones para cumplir con las regulaciones gubernamentales de seguridad informática en sus organizaciones y que deberán observar si desean crecer internacionalmente. Por último se explican brevemente algunos estándares internacionales de gestión de las Tecnologías de la Información los cuáles nos ayudarán a entender mejor el porqué de la realización de ésta tesis.

El capítulo 4 se expone el estándar ISM3, realizando una explicación más detallada de cada una de las fases que se deben realizar para su implementación dentro del Departamento de Seguridad de Cómputo de la Facultad de Ingeniería (DSC-FI).

El capítulo 5 explica brevemente la función del DSC-FI dentro de la Facultad de Ingeniería y posteriormente la ejemplificación de implementación del ISM3 con base en el proceso más importante del DSC-FI.

Finalmente se exponen las conclusiones de éste trabajo así como las recomendaciones que se pueden realizar a futuro dentro del Departamento de Seguridad con base en el uso del ISM3 como gestor de procesos de seguridad informática.

OBJETIVO

Definir el modelo de gestión que el Departamento de Seguridad en Cómputo de la Facultad de Ingeniería deberá adoptar en sus procesos, para una administración eficaz de sus recursos y actividades, que permita fortalecer las tecnologías de información y los procesos soportados por ellas, conforme a la misión de seguridad informática del Departamento y de la Institución.

CAPÍTULO 1

SEGURIDAD EN LAS ORGANIZACIONES

Las organizaciones continuamente se ocupan por ser mejores día a día y tratan constantemente de ir a la vanguardia en lo que respecta a las Tecnologías de la Información. De ésta manera creen que pueden sobresalir de otras, sin embargo aun no es una práctica común el que tomen en consideración un aspecto tan crítico e importante como lo es la seguridad a fondo en todos sus ámbitos.

No solo hablamos de la seguridad física sino también de aquella que es intangible. Muchas veces es la que menos se puede medir y en consecuencia es imposible saber las pérdidas que ha tenido la organización en ese rubro.

La seguridad en la organización no se puede medir por la tecnología con la que cuenta sino por la importancia de ésta a través de los procedimientos y servicios que le permiten funcionar adecuadamente. No es una tarea sencilla el medir ese grado de seguridad sin embargo un buen punto de partida es responder a las siguientes preguntas: ¿Qué se quiere proteger?, ¿Porqué?, ¿De qué o quién? y ¿Cuándo?

1.1 Fundamentos

Este primer capítulo nos presenta una introducción sobre la seguridad informática, así como conceptos importantes, los cuales serán la base para entender mejor los capítulos posteriores.

Cuando se hable de activos se entenderá que son todos aquellos elementos requeridos para la operación de la organización, estos se refieren a la información (electrónicos, papeles), sistemas (procesos y bases de datos), software (aplicaciones y servicios) y hardware que están dentro de la entidad.

1.1.1 Concepto de la seguridad informática

La seguridad informática se puede definir como el conjunto de herramientas, procedimientos, técnicas y reglas que nos ayudan a proteger los sistemas informáticos y de esa manera garantizar la confidencialidad, autenticación, integridad, no repudio, control de acceso y disponibilidad de la información.

La seguridad informática no se ocupa solamente en hacer una configuración de firewall, aplicar parches que solucionen huecos de seguridad o instalar un antivirus, la seguridad informática es determinada en función de qué necesitamos proteger y porqué, de qué es necesario proteger, y cómo protegernos durante el tiempo de vida de nuestros activos.

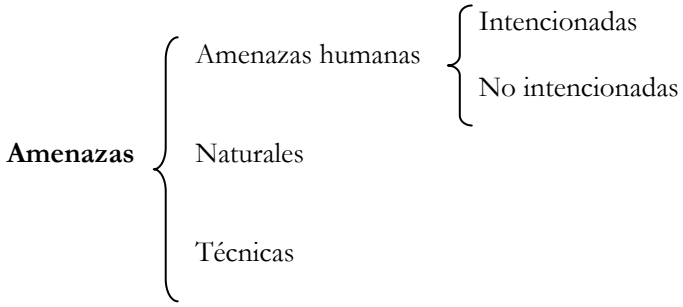
1.1.1.1 Vulnerabilidad

El mejor concepto que podemos encontrar de la vulnerabilidad se refiere a una debilidad, la cual posibilita que una amenaza se realice y termine en un problema de seguridad. La relación entre vulnerabilidad y amenaza es muy amplia ya que si no existe una de ellas la otra por consecuencia tampoco. Por lo general las vulnerabilidades pueden prevenirse siempre y cuando sean conocidas, de otro modo están latentes en el sistema.

1.1.1.2 Amenaza

Una amenaza es una acción que atenta y viola la seguridad realizando un impacto indeseable en el sistema efectuado por un evento o una persona. Las amenazas aprovechan una vulnerabilidad para cumplir su objetivo produciendo daños a nuestros activos.

Existe una clasificación de amenazas:



Las amenazas humanas a su vez se dividen en dos: **Las intencionadas** son realizadas por personas que no están autorizadas para entrar al sistema ya sea a la información intangible o los lugares físicos de la organización y a su vez utilizan de forma indebida los recursos. **Las no intencionadas** son ocasionadas o vienen de la mano por la ignorancia y negligencia de las personas que tienen relación directa o indirectamente con el sistema.

Las naturales son aquellas situaciones que están fueran del alcance humano por ejemplo los terremotos, incendios, inundaciones, relámpagos, etc.

Por último las **amenazas técnicas** son fallos de los equipos, descargas eléctricas entre otros factores los cuales pueden ocasionar pérdidas de equipos o de información.

Las amenazas humanas intencionadas pueden clasificarse aún más dependiendo el fin malicioso que persigan, este tipo de amenazas son: la intercepción, interrupción, modificación y fabricación los cuales se explican más adelante.

1.1.1.3 Ataque

Es la acción de una amenaza cuya finalidad es interrumpir, negar o destruir toda información y/u operación de los equipos y redes de cómputo. Cuando ésta acción se realiza se violan los sistemas y mecanismos de seguridad del sistema impidiendo el buen funcionamiento de éste.

Los ataques se pueden clasificar en pasivos y activos. Los pasivos son aquellos que no modifican el estado del sistema mientras que los activos sí lo alteran.

1.2 Objetivos de la seguridad informática

Una organización siempre tendrá información importante que desea cuidar y proteger, debido a esto nace la Seguridad Informática la cual abarca una extensa área y se dedica a velar por la seguridad de la información de la organización.

Dentro de los objetivos corporativos podemos definir los siguientes, algunos de los cuales son dependientes de los procesos de seguridad:

- Mantener la reputación de la organización y sus productos.
- Lograr sus objetivos.
- Permanencia.
- Cumplimiento con contratos y regulaciones.
- Prevenir robo, fraude y corrupción.
- Prevenir huecos en acuerdos contractuales.
- Proteger los derechos incluyendo la privacidad.
- Protección a los derechos reservados.
- Proteger la privacidad de los clientes.

Dado lo anterior podemos decir que la Seguridad Informática juega un papel relevante en el cumplimiento de los objetivos señalados para cualquier organización, buscando no solo la prevención de problemas de seguridad sino catapultando el potencial organizacional al entender y aceptar la importancia de tener controles, acciones, procedimientos, etc., que regulen el buen funcionamiento de los activos y el personal.

Una empresa puede tener diferentes objetivos de seguridad dependiendo de su localización geográfica o sus líneas de negocios o servicios.

1.2.1 Compromisos de la seguridad informática

Cuando una organización busca tener seguridad, sabe que tiene que adoptar ciertas responsabilidades y obligaciones no solo contractuales si no también legales y hasta en ámbitos internacionales para llevar a cabo todos sus procesos.

Pero esto no es algo imposible sino que se necesita que todos los involucrados se comprometan a llevar a cabo sus tareas, conocer las políticas y normatividades organizacionales, conocer las disposiciones legales en cuanto a la regulación informática de los países donde tiene convenios, invertir adecuadamente en capacitación y dispositivos que ayuden a mitigar los riesgos informáticos y principalmente comprender la importancia de la seguridad informática como uno de los elementos más importantes para la prestación de servicios.

1.2.2 Servicios de la seguridad informática

La seguridad informática tiene servicios que son fundamentales para un buen funcionamiento y accionar. Estos conceptos son básicos en un sistema, si no se está aplicando uno de éstos quiere decir que aún no existe una infraestructura de seguridad sólida en la organización.

1.2.2.1 Confidencialidad

Es un servicio de seguridad que tiene como finalidad el mostrar la información del sistema, para que ésta sea utilizada, manejada y modificada únicamente por el proceso o personal autorizado.

1.2.2.2 Autenticación

Es el procedimiento a través del cual permite que los procesos o usuarios se puedan identificar y además verificar que son quienes dicen ser para posteriormente utilizar los recursos del sistema.

1.2.2.3 Integridad

Es muy importante proteger la información, datos o sistemas y encontrarlos siempre completos es por eso que se encuentra la integridad, ésta propiedad garantiza que la información no será modificada, alterada, copiada o destruida durante su almacenamiento o proceso de transmisión por personal no autorizado.

Asegurar que la información almacenada o transmitida no puede ser corrompida, ni falseada ya sea intencional o accidentalmente es el objetivo de la integridad, que los datos recibidos o recuperados son exactamente los enviados o almacenados.

1.2.2.4 No repudio

Otro problema de seguridad se desarrolla cuando existe una comunicación entre entidades y alguna de las partes o ambas niega haber entablado una conexión entre ellas. Para este problema existe un servicio de seguridad llamado No repudio donde el emisor recibe la confirmación de la entrega y el receptor tiene comprobante de la identidad del remitente y de esta manera no podrán negar ninguna de las dos partes, que hubo una comunicación.

1.2.2.5 Control de acceso

El control de acceso es un mecanismo que permite solo al personal autorizado acceder a los activos, es decir a los recursos, datos o sistema permitidos. Además de ser utilizado para autenticar las capacidades de la organización con la finalidad de asegurar los derechos que se tienen para entrar a los recursos que posee. Todo esto lo realizan por medio de una verificación y autorización, es decir, la verificación nos asegura la identidad del proceso o usuario que está solicitando el acceso mientras la autorización limita la información o recursos que puede utilizar.

1.2.2.6 Disponibilidad

La disponibilidad es la seguridad que da a los usuarios, servicios o procesos de que puedan acceder y utilizar los activos del sistema en el momento que lo requieran. Dentro de este servicio podemos decir que el hardware y software se mantienen funcionando eficientemente y en caso de alguna falla es capaz de recuperarse fácilmente. Con este concepto se puede ver la continuidad operativa de la organización.

Cuando es atacada la disponibilidad se puede realizar una negación de servicios conocida como *Denial of Service* (DoS) o como comúnmente decimos "tirar" el servidor. Esto afecta mucho a la organización puesto que se pierde productividad o credibilidad.

1.3 Amenazas deliberadas a la seguridad en las Tecnologías de la Información

Como se vio anteriormente la amenaza es una acción que puede producir una violación en la seguridad. Existen tipos de amenazas que afectan los sistemas informáticos explotando las vulnerabilidades que hay dentro de la organización.

- Amenazas deliberadas a la seguridad en las Tecnologías de la Información
  - Interrupción
  - Intercepción
  - Modificación
  - Fabricación
  - Ataques pasivos
  - Ataques activos
    - Suplantación de identidad
    - Reactuación
    - Modificación de mensajes
    - Degradación fraudulenta del servicio

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente a un destino.

1.3.1 Interrupción

La interrupción se realiza cuando un recurso del sistema es perturbado por otro de tal manera que llega a ser destruido, no disponible o inoperable. Con esto podemos decir que se realiza un ataque en contra de la disponibilidad del sistema. (Fig. 1.1)

El resultado de éste acto puede ser la destrucción maliciosa del hardware o software como es el borrado de programas, registros, bases de datos o información del sistema, también puede ocasionar el mal funcionamiento de éste.

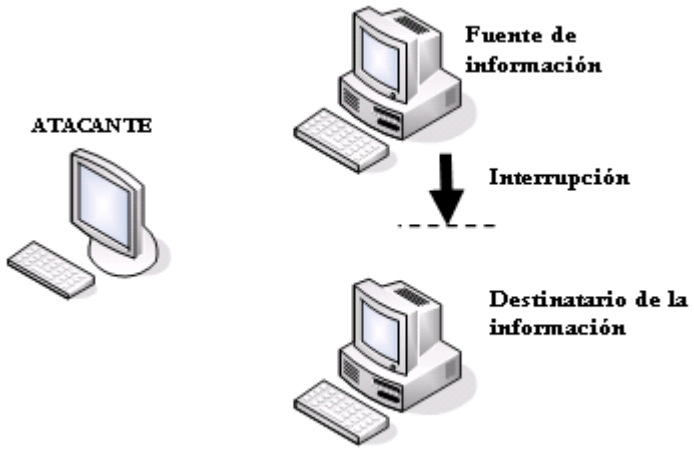


Fig. 1.1 Interrupción

1.3.2 Intercepción

Ésta se presenta cuando un tercero no autorizado, el cual puede ser una persona o programa, logra acceder a un recurso del sistema y utilizarlo. (Fig. 1.2)

Podemos decir que uno de sus objetivos es intervenir sin alguna autorización en el análisis de tráfico o en la comunicación de datos que exista entre los recursos del sistema o de los usuarios. Algunos ejemplos sobre éste problema sería obtener datos por medio de programas realizados previamente, copia ilícita de la información del sistema así como de archivos o programas que se encuentren en él. Pero algo muy común es el interferir en la red de comunicaciones para obtener la información sin que se den cuenta los demás de lo que está sucediendo.

Éste tipo de ataque perturba la confidencialidad del sistema. Además de ser el más difícil de localizar ya que no produce ninguna alteración y no se sabe en que momento puede resultar peligroso.

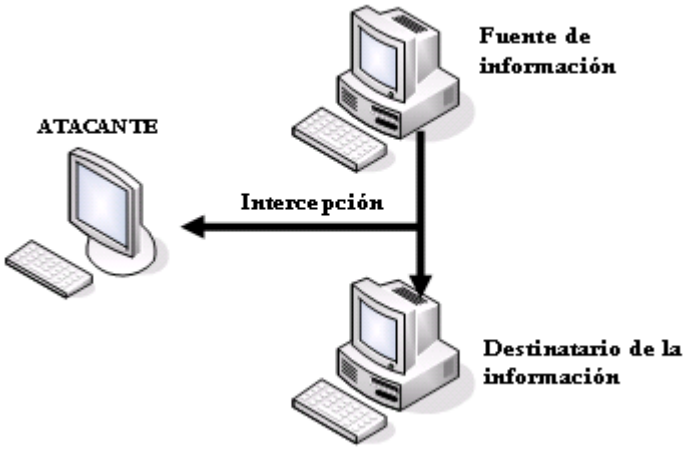


Fig. 1.2 Intercepción

1.3.3 Modificación

Consiste en la alteración de la información de un sistema, primero logra acceder y ya dentro de éste de manera maliciosa empieza a cambiar la información o bien a manejarla a su beneficio. (Fig. 1.3) Éste ataque es el más peligroso debido a lo importante que es la información y la cual no será recuperada sino se hizo anteriormente una prevención sobre el asunto (en este caso sería el respaldo de la información).

Ejemplos de este ataque podría realizarse con la ejecución de código malicioso (virus o troyanos) dentro del sistema el cual fue instalado sin la autorización de la gente responsable, también podría ser la alteración de programas para que éstos realicen otras funciones, la modificación de bases de datos o información que se esté transmitiendo.

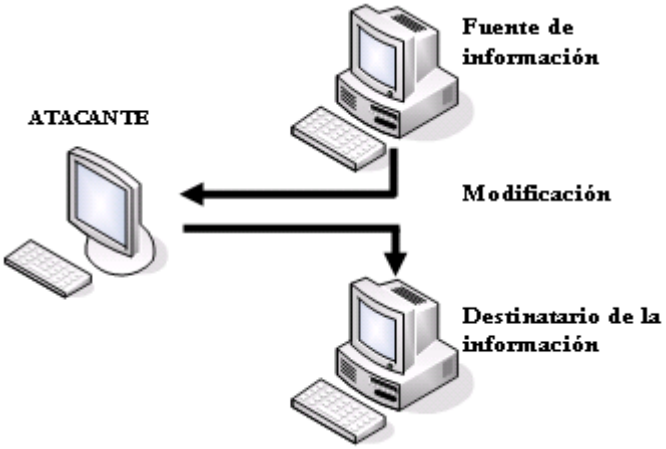


Fig. 1.3 Modificación

1.3.4 Fabricación

Este ataque se realiza a través de un tercero, el cual produce información falsa y la introduce en los sistemas (Fig. 1.4). Atenta contra la autenticidad de los sistemas.

Ejemplos de este ataque son la inserción de mensajes falsos en la red o añadir registros a un archivo, incluir programas, etc.

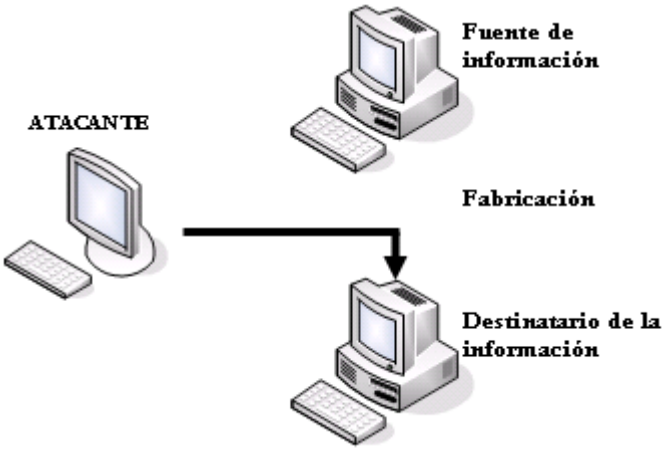


Fig. 1.4 Fabricación

1.3.5 Ataques pasivos

Este tipo de ataque es uno de los más peligrosos ya que actúa de una manera silenciosa, la cual hace que sea difícil de detectar, el ataque no altera la comunicación en el caso de intervenir en una, sino que solo la monitorea con el propósito de obtener la información para después utilizarla y causar daños.

Sus principales objetivos son la intercepción de datos y el análisis de tráfico. La intercepción de datos la realiza el atacante para el entendimiento de la información y de esa manera identificar si es importante o no, ayudándose con el análisis de tráfico ya que con éste se observa toda la actividad que se está realizando y por ende la información que está transmitiéndose.

1.3.6 Ataques activos

Los ataques activos realizan algún tipo de modificación, alteración o creación falsa de datos o mensajes. Estos ataques se dividen en cuatro categorías

- Suplantación de identidad
- Reactuación
- Modificación de mensaje
- Degradación fraudulenta del servicio

1.3.6.1 Suplantación de identidad

Es la técnica donde el intruso se hace pasar por un usuario o proceso y de esa manera accede a los recursos de un sistema. Este tipo de ataque necesita ir acompañado de otro para que tenga éxito.

1.3.6.2 Reactuación

Este ataque se lleva acabo cuando uno o varios mensajes de un sistema son capturados y repetidos lo cual causa un efecto no deseado.

1.3.6.3 Modificación de mensajes

Durante la transmisión de mensaje o datos, éstos son interceptados para ser alterados, retardados o reordenados y de esa forma no llegan a su destino de la manera en que el sistema lo deseaba.

1.3.6.4 Degradación fraudulenta del servicio

Cuando se realiza este ataque el buen funcionamiento del sistema es afectado ya que impide el uso normal de los recursos del sistema. Logrando por ejemplo una denegación de servicio.

1.4 Cultura de la seguridad informática en las organizaciones

Siempre existe el riesgo de sufrir algún daño o pérdida en nuestros activos, por lo que se debe estar siempre alertas ante tal situación. La infraestructura de seguridad no sirve de nada sino se cuenta con una correcta administración, por eso es importante contar con el personal calificado que lleve a cabo estas tareas.

Se necesita fomentar una cultura en el personal que está involucrado en cada una de las tareas de la organización en lo que se refiere a la seguridad, ya que si no existe éste conocimiento los riesgos pueden causar un impacto negativo.

La comunicación y manipulación que exista entre el personal y los activos es muy importante porque conocerán a fondo cada una de sus vulnerabilidades y sabrán como resolverlas si existiera algún problema.

1.4.1 Seguridad física

Dentro de una organización se necesita tener ciertas prevenciones para proteger no solo lo intangible sino también todo lo físico. Para esto se necesitan ciertas medidas de seguridad física, que permitan minimizar los riesgos existentes. De ésta manera se deben contemplar todos aquellos problemas que afecten nuestros activos.

Las medidas de seguridad física se dividen en dos clases las cuales son: las ambientales por ejemplo las inundaciones, de humedad, incendios, el calor, el frío, fallas eléctricas, tormentas eléctricas, etc. y las interferencias humanas ya sean intencionadas o accidentales.

Para los factores ambientales las medidas que se pueden realizar dependen mucho del lugar donde serán utilizadas además de la tecnología que se está resguardando.

La gran mayoría de sistemas son alimentados por electricidad por lo que existe la posibilidad de que ocurran fallas las cuáles pueden ocasionar descargas eléctricas, hasta la pérdida del equipo, por lo que se necesita tener siempre un buen respaldo y suministros de energía de reserva.

En lo que respecta a la seguridad del equipo debe estar protegido del clima para que las temperaturas extremas o la humedad no afecten su actividad, ya que debe tener un clima estable y de esa manera su funcionamiento y tiempo de vida sean los más óptimos, otra cosa importante es no permitir que el polvo y humo afecten los sistemas, por ejemplo muchas veces el residuo del cigarrillo puede dañar los equipos, o la falta de limpieza en las áreas de trabajo pueden acumular el polvo.

Es recomendable que haya un cierto grado de humedad pues si el ambiente es muy seco existe mucha electricidad estática pero también no debe haber un extremo pues si se tiene un nivel de humedad muy elevada puede producir una condensación en los circuitos integrados y esto de cómo consecuencia un cortocircuito.

Tenemos que tomar en consideración que los desastres naturales pueden tener grandes consecuencias si no los tomamos en cuenta además que son difíciles de pronosticar.

Otro aspecto importante es el equipo de comunicación que requiere de una seguridad física especial. Para tener una comunicación se requiere de una conexión de red que en muchas ocasiones utiliza el sistema de cableado el cual debe ser protegido ya que éstos pueden ser destruidos por roedores o humanos.

Una de las maneras de tomar medidas de seguridad para los factores humanos es aislar todo lo físico para que no esté al alcance de cualquier persona, con esto limitamos nuestros sistemas y restringimos el personal que puede utilizarlo pero también existen aquellos problemas que son accidentales y difíciles de prevenir. Si el atacante tiene acceso físico a los equipos, las demás medidas de prevención resultan inútiles. La forma en que podemos restringir los accesos es a través de dispositivos sofisticados que restringen la entrada a las áreas donde se encuentra la tecnología. Por ejemplo podemos tener desde los más sencillos como son los candados, cerrojos hasta llegar a los más modernos como son los cerrojos que acceden por medio de códigos de acceso, como son tarjetas, huellas dactilares, de mano o retina, entre otros.

Otra manera de proteger el lugar podría ser por medio de vigilancia a través de guardias de seguridad para controlar el acceso al personal. Además de utilizar cámaras de seguridad y de ésta manera se monitorea todas las áreas que se desean vigilar. También tenemos que tener presente y llevar un

control de quienes tienen acceso y quienes no, además de saber quienes han ingresado al lugar y por cuánto tiempo permanecieron en el.

Al tener todo este tipo de prevenciones y detecciones como es el acceso controlado con ciertas políticas, el uso del equipo solo por personal autorizado y que tenga conocimientos sobre lo que está manejando, respaldos sobre la información, etc. se puede tener medidas óptimas que nos den una adecuada seguridad física.

1.4.2 Seguridad en Tecnologías de la Información

Las Tecnologías de la Información es un término muy amplio ya que son herramientas y metodologías que abarcan tanto los aspectos de administración y procesamiento de la información. Comprende todas las tecnologías basadas en las computadoras y comunicaciones las cuales nos ayudan a obtener, almacenar, manejar y transmitir información. En la actualidad las empresas han tomado en cuenta esta parte creando departamentos de TI ya que esto permite a la organización mejorar su administración e integración de las necesidades informáticas en todas las áreas funcionales de la misma. Además que las TI se han convertido en algo fundamental y en cierta forma hasta normal en la vida cotidiana del ser humano

Se necesita de gente profesional que ayuden a diseñar, desarrollar, mantener y administrar tanto software, hardware y redes informáticas, ya que son elementos necesarios para el proceso de TI. Las TI no corrigen procesos mal diseñados sino que ayuda a tener un mejor desempeño.

Cuando hablamos de tecnología envolvemos varios aspectos, ya que hablamos de procesos los cuáles involucran técnicas, conocimientos científicos, empíricos y aspectos económicos. Por lo que las organizaciones consideran importante invertir en tecnología por muchas razones como: agilizar procesos, reducir costos, responder a los cambios del entorno, darle al cliente, justo lo que pide y encontrar un diferenciador frente a la competencia.

Para tener en la organización Tecnologías de Información se requiere una persona especializada en ésta área para no caer en problemas que hagan ver como si no sirvieran las tecnologías. A continuación se describirán algunos errores que comenten las organizaciones al adquirir tecnología por no tener una visión correcta:

- No hacer un análisis, es decir, no se define en donde se debe aplicar la tecnología, con qué finalidad, cuáles serán los problemas a resolver y hasta dónde se quiere llegar, antes de proceder.
- Otro caso muy usual sucede cuando se adquieren primero las herramientas y después se tratan de ajustar a éstas los procesos internos, las metas y los alcances organizacionales, sobre la marcha, se está cometiendo un grave error, pues lo mas adecuado es hacerlo justamente a la inversa, es decir, adaptando la tecnología a los procesos de negocio y logísticos de la organización, es decir, quieren tomar la tecnología como fin y no como medio además que no alinean la tecnología con los objetivos del negocio.
- Utilizan las TI como "una moda" o para mantenerse a la vanguardia sin estar seguros si la adquisición resultará útil o si impactará de manera positiva a la organización.
- Compran o cambian sus tecnologías solo por imitar a la competencia, lo cual los lleva a invertir en cierta tecnología sólo porque al otro le ha funcionado bien, sin considerar que cada empresa vive dinámicas distintas y maneja un sistema diferente.
- No se prepara un ambiente que ayude a recibir las herramientas, cosa importante ya que tiene que tomarse en cuenta a los empleados, y a los clientes.

- Se debe tomar en que tan complicado resultará su implementación, ya que algunas aplicaciones a veces no se comunican con las que ya están implementadas y se tiene que gastar más de lo previsto para que se puedan acoplar entre ellas.
- Por último y uno de los mas importantes es que se olvidan de la seguridad. Este punto es muy importante por que la seguridad es un elemento que puede costar muy caro dada la complejidad de las amenazas y vulnerabilidades cibernéticas y el auge que ha tomado Internet, por lo que cualquier nuevo desarrollo tecnológico debe contemplar cómo prevenir los posibles ataques de malware, *phishing*, , *spam*, robo de identidad, etc.

Entrando al tema de la seguridad, sabemos que las TI son muy buenas y robustas pero también las amenazas son un tanto más peligrosas. Ya que los ataques que se hacen a las empresas no son sólo un simple juego sino que si son bien dirigidas y ejecutadas profesionalmente pueden terminar en la obtención de ganancias financieras. Lo cual alerta a las organizaciones a buscar maneras de protegerse de aquellos daños que podrían ser irrevocables. Es por eso que las empresas deben entender que la seguridad es algo inherente en la infraestructura de las Tecnologías de la Información y de esa manera bajar al máximo las vulnerabilidades.

Deben asegurarse de tener una estrategia de seguridad completa, que abarque tecnologías de punta, procesos bien establecidos y recursos humanos: manuales, capacitación. La mejor estrategia de continuidad puede fallar si el personal no sabe qué puede y qué no puede hacer, o cómo debe actuar en caso de presentarse un incidente que comprometa la operación de la organización.

En la actualidad existe un gran número de vulnerabilidades y el costo de los incidentes siguen incrementándose, lo cual puede ser resultado de que la mayoría de los departamentos TI no prueban adecuadamente las aplicaciones que se utilizan en la organización, como es el encontrar las fallas de seguridad durante el ciclo de vida de las mismas. Pero esto se debe a una falta de conocimiento en el personal, hoy en día se han sumado más riesgos ya que las empresas cuentan con protección perimetral a través de firewalls, detección de intrusos (IDS, por sus siglas en inglés) de switches y ruteadores que en muchos casos no son administrados adecuadamente, adicionalmente los intrusos han buscado nuevas maneras para infiltrarse y esto a llevado a atacar vulnerabilidades en el software de formas novedosas y hasta de manera comercial, por lo que los desarrolladores deben de estar conscientes del problema al que se enfrentan.

Es importante educar a la organización acerca de lo que es importante y por qué, así como quiénes son los responsables de las diferentes tareas, de esta manera se define la estrategia y las reglas de seguridad a seguir lo que generará un proceso de inspección y análisis. Una de las responsabilidades del personal de TI es monitorear, controlar y resolver fallas designando un lugar para proveer múltiples aplicaciones con altos niveles de monitoreo. A través de ellos se controlan y distribuyen las aplicaciones e información de una organización.

Un buen diagnóstico de la seguridad en la empresa permitirá obtener en un tiempo reducido el estado actual de la seguridad de la información a nivel organizacional, bajo un análisis que considere redes y comunicaciones, aplicaciones críticas, manejo de la información (en medios electrónicos o documentales), estrategia y objetivos de seguridad, contenido y alcances de las políticas de seguridad establecidas, así como la seguridad física.

El factor humano es la parte más delicada, ya que no existe ningún sistema ni aplicación que no dependa de las personas. Esto hace vulnerables a todas las organizaciones independientemente del software y equipo de seguridad de que dispongan. Ignorar o malentender la importancia y valor de la información, representa en sí mismo una amenaza a la continuidad. La seguridad de la información debe estar orientada a la continuidad y capacidad competitiva de las organizaciones, por lo que todas las

áreas deben involucrarse en ella, desde los niveles ejecutivos más altos, llámese Gerente General, Director, Presidente, etc., hasta los niveles operativos y menores en la jerarquía de la organización.

Por último las demandas actuales de TI requieren la convergencia de técnicas, herramientas y conocimientos que aseguren la mayor aportación de valor a los servicios al tiempo de minimizar los riesgos que conlleva el uso de la tecnología.

1.4.3 Administración de riesgos

En cualquier ámbito será importante manejar una serie de herramientas que nos ayuden a garantizar una correcta evaluación de los riesgos que se encuentran dentro de la organización. Para saber como administrar los riesgos es importante tener en cuenta primeramente que es un riego. El riesgo frecuentemente se relaciona a la probabilidad que un evento no deseado ocurra y éste tenga consecuencias no favorables a la organización. Cuando hablamos de riesgo informático nos referimos a la probabilidad de que exista una amenaza, la posibilidad de tener vulnerabilidades dentro del sistema (debilidades) y de esta manera generar un impacto desfavorable. Algo muy cierto es que los riesgos siempre existirán pero es conveniente conocerlos y de ésta manera estar preparados para manejarlos y resolverlos.

Existe diferentes tipos de riesgos los cuales los podemos clasificar en:

- Riesgo financiero: El riesgo financiero envuelve la relación entre una organización y una ventaja que puede ser perdida o perjudicada.
- Riesgo dinámico: Son el resultado de cambios en la economía ya sean internos o externos a la organización.
- Riesgo estático: Estos riesgos surgen de otras causas distintas a los cambios de la economía tales como: deshonestidad o fallas humanas.
- Riesgo especulativo: Describe una situación que espera una posibilidad de pérdida o ganancia. Un buen ejemplo es una situación aventurada o del azar.
- Riesgo fundamental: Envuelve las pérdidas que son impersonales en origen y consecuencia. La mayor parte son causados por fenómenos económicos, sociales. Desempleo, guerra, inflación, terremotos son todos riesgos fundamentales.
- Riesgo particular: Son pérdidas que surgen de eventos individuales antes que surjan de un grupo entero; el incendio de una casa y el robo de un banco son riesgos particulares.

Pero no son los únicos riesgos, también existen los riesgos relacionados con la informática los cuales se clasifican en:

- Riesgos de Integridad: En esta parte son los riesgos asociados con la autorización y exactitud de la entrada, procesamiento y reportes de todas las aplicaciones utilizadas en la organización.
- Riesgos de relación: Se refiere al uso de la información creada por una aplicación de la organización.
- Riesgos de acceso: Aquellos riesgos que existen al hacer un inapropiado acceso a un sistema, datos e información.
- Riesgos en la infraestructura: Son todos aquellos riesgos que vienen de una mala estructura tecnológica dentro de la organización.

- Riesgos de seguridad general: Son todos los riesgos relacionados con los accidentes dentro de la organización ya sean físicos o intangibles.

Después de tener un amplio concepto de que es un riesgo y sus clasificaciones podemos decir que la administración de riesgos es una aproximación del comportamiento de los riesgos, anticipando posibles pérdidas accidentales creando un diseño e implementación de procedimientos para minimizar las pérdidas y el impacto económico que pudiera ocurrir en la organización.

Necesitamos tener un proceso de la administración de riesgos, lo primero que debemos de hacer es determinar los objetivos, es decir la manera en que se va a llevar acabo el programa de administración de riesgos. Posteriormente se lleva acabo un análisis profundo dentro de la organización para poder identificar los riesgos que se encuentran dentro de ésta, ya que cada una de las organizaciones se maneja diferente y por lo tanto se tienen diferentes riesgos. Pero no es una tarea difícil ya que existen herramientas que nos ayudan a identificarlos. Ya identificados los riesgos se hace una evaluación profunda para clasificarlos de mayor a menor, es decir, existen riesgos críticos, importantes y no importantes y dependiendo de esto es como se les pone mas atención a aquellos que más lo requieren. Cuando ya tenemos clasificados los riesgos dentro de la organización se debe considerar alternativas y procedimientos para tratar los riesgos, de ésta manera se realizan métodos que nos ayudan a evitar los riesgos si es posible o en su defecto retenerlos o reducirlos. Y por ultimo se tiene que tener una constante revisión de los riesgos ya que la organización va cambiando constantemente y pueden surgir nuevos que se deben contemplar así como pueden existir otros que desaparezcan conforme crece la empresa.

Cuando tenemos una correcta administración de riesgos se utilizan ciertas técnicas o herramientas que nos ayudan a su funcionamiento.

- Control de Riesgos: Ésta técnica es diseñada para minimizar los posibles costos causados por los riesgos a que esté expuesta la organización.
- Financiación de Riesgos: Financiación es garantizar la habilidad de conocer recursos financieros y las pérdidas que pueden ocurrir en ellos.

1.5 Delito informático

Cuando hablamos de leyes y derechos debemos tener algunos conceptos claros y precisos ya que son el fundamento para definir el delito informático.

Primero debemos saber que derecho es un "conjunto de reglas de conducta externa del sujeto, en sus relaciones con los demás, enunciadas por los órganos competentes e impuestas coactivamente a los ciudadanos".

Otro de los conceptos importantes es el de las normas ya que el derecho es un conjunto de normas jurídicas las cuales son reglas u obligaciones para todos los ciudadanos.

Las tecnologías de la información han avanzado cada día lo cual ha abierto nuevas puertas para infringir la ley, aunque también se empiezan a cometer delitos tradicionales de una manera nueva utilizando la informática. Primeramente definamos el concepto de delito: el cual es una conducta normalizada por la ley, antijurídica, culpable y censurable la cual es penada.

En la actualidad todos podemos ser víctimas de delitos entre ellos están los informáticos. Desgraciadamente estos delitos no han sido valorizados por las leyes y algunos de ellos quedan impunes.

El concepto de delito informático engloba varios aspectos, ya que no sólo estamos hablando de aquellos delitos donde se atenta en contra de sistemas sino que también nos habla de aquellos delitos que se realizan mediante el uso de un sistema.

El delito informático es cualquier acto ilícito penal (las cuales deben ser sancionadas por el derecho penal) en el que está involucrada la informática y sus técnicas; que desempeñan un papel muy importante para realizar los delitos. Las computadoras son utilizadas como instrumentos o fin para realizar los delitos, es decir son el material u objetivo a atacar. Si bien cabe destacar que no son las computadoras las que realizan los actos sino el hombre que las utiliza para hacer sus actos ilícitos.

Existen dos tipos de sujetos involucrados en los delitos:

Sujeto Activo: Son aquellos sujetos que realizan el delito informático. Una de las características importantes de estas personas es que poseen un gran conocimiento y habilidad sobre el manejo de la informática. Muchas veces estas personas no se encuentran en el lugar donde comenten los delitos y esto les ayuda a no ser capturados tan fácilmente. A éste tipo de personas la sociedad no los considera como delincuentes ni son rechazados ya que no sea valorizado el delito informático como algo malo.

Sujeto Pasivo: Es la victima del delito en la cual recae la acción que hace el sujeto activo. La víctima no sólo puede ser una persona sino también instituciones u organizaciones que tienen sistemas informáticos.

Los delitos informáticos se pueden clasificar con 2 categorías.

1.- Sea utilizado como instrumento, es decir que la tecnología sea manejada como medio o método para realizar el delito.

2.- Sea utilizado como fin, el resultado del delito informático recae en alguna computadora o sistema al cual se le hace el daño.

También tenemos algunos tipos de delitos. Es difícil calcular un número exacto de ellos:

El **Fraude Informático** lo podemos ver en la intervención de los datos de entrada al sistema, modificaciones o reproducción no autorizadas en los programas, modificación fraudulenta de la información almacenada en el sistema, intervención en la líneas de transmisión de datos, falsificación informática, entre otras. Este tipo de delito es muy amplio ya que depende mucho del ingenio que existe en los delincuentes para llevar a cabo sus actos ilícitos.

Acceso no Autorizado se realiza cuando se entra a un sistema informático sin la autorización del dueño ya sea por mera curiosidad o para realizar sabotaje dentro del sistema.

La **Destrucción de datos** se realiza cuando se causan daños al sistema muchas veces esto se realiza por medio de virus, gusanos, caballos de Troya, etc.

Cuando hablamos de **infracción de los derechos de autor** se refiere a la copia, distribución, destrucción y manipulación sin tener permisos del creador de dicho sistema.

La **infracción del Copyright de Bases de Datos** se refiere a los datos que se encuentran dentro de la base y que son utilizados.

Otro problema grave es cuando se realiza la **intercepción de e-mail**, ya que leen información que puede ser confidencial y algunas veces la modifican o la destruyen para que no llegue a su destino.

Las **estafas electrónicas** es un caso que se ha hecho muy común en la red, ya que las personas han optado por utilizar las compras vía Internet donde son engañados para que estos den sus números de cuentas o ingresen dinero a lugares que no conocen y de esa manera son chantajeados para perder su dinero.

Por último en la **transferencia de fondos** no se produce un engaño a alguna persona sino a sistemas.

Los delitos informáticos son difíciles pero no imposibles de descubrir, el problema es que muchas veces no son denunciados a las autoridades y por otro lado existe una ignorancia dentro de las leyes las cuales no protegen a las víctimas ya que no existe de parte de las autoridades un interés, comprensión, investigación y aplicación de las leyes en este ámbito.

CAPÍTULO 2

PROCESOS DE PLANEACIÓN Y ADMINISTRACIÓN DE SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN

Este capítulo nos permitirá comprender la estructura que debe desarrollarse en la organización para tener un adecuado plan de administración de seguridad en las Tecnologías de la Información (TI); de ésta manera se establecerá un fundamento sólido a través del cual se formen cimientos para que la organización crezca en todas las áreas junto con las TI y la seguridad que se requiere. Cuando hablamos de procesos se engloban cuatro conceptos: la planeación, prevención, detección y reacción.

La planeación y administración de seguridad en TI, son todos los procesos para desarrollar y mantener un programa de seguridad dentro de la organización. Es importante que todas las actividades y funciones identificadas en la Fig. 2.1 se encuentren alineadas al estilo, tamaño y estructura de la misma.

La seguridad como tal tiene un proceso continuo el cual podemos ver en el siguiente diagrama:

Fig. 2.1 Actividades y funciones de la Seguridad

El punto de inicio es establecer una clara visión de los objetivos de seguridad de la organización; estos objetivos son delineados por otros superiores y dirigen las estrategias e iniciativas de seguridad en TI.

De esta forma, la definición de las políticas de seguridad en TI son creadas tomando en cuenta la estructura organizacional.

2.1 Planeación en el manejo de la seguridad en Tecnologías de la Información

En la actualidad las Tecnologías de la Información son sumamente dinámicas, es decir, el cambio es constante, por tal razón siempre que se introducen debemos crear un plan para tener buenos resultados. La planeación permite asimilar los cambios para decidir las acciones que deben realizarse en un futuro; durante el proceso se toman en cuentan diferentes alternativas y se elige la mejor.

Es un sistema donde primero se definen los objetivos y sus metas para posteriormente desarrollar las políticas, estándares, guías básicas y procedimientos los cuales serán dinámicos durante su transcurso de vida para adaptarse a cualquier cambio.

Es importante tener una planeación del manejo de las TI ya que propicia el desarrollo de la organización, reduce los niveles de incertidumbre, prepara a la entidad para hacer frente a las contingencias, mantiene una visión mas elevada con un afán de lograr y mejorar las cosas, establece un sistema racional para la toma de decisiones, reduce al mínimo los riesgos y aprovecha las oportunidades que se le presenten, elimina la improvisación, proporciona al personal mejores rendimientos de tiempo y esfuerzo y permite al ejecutivo evaluar diferentes alternativas antes de tomar alguna decisión. La planeación y el desarrollo de cada una de las etapas de acuerdo a un modelo, responsabilidad, cumplimiento de normas, disciplina y ética ayudarán a la organización a crecer.

Algo muy importante es que la planeación de la seguridad debe siempre alinearse a los objetivos de la organización.

2.1.1 Compromiso ejecutivo

Durante la vida de una organización se realizan esfuerzos para definir sus directrices de seguridad y concretarlas, para esto se necesita una gran labor de convencimiento a los directivos, hacerles ver la necesidad de crear el mejor proceso de seguridad para las TI. Pero muchos de estos inconvenientes inician por los tecnicismos informáticos y por la falta de estrategia de los especialistas en seguridad.

Es muy importante contar con una persona especialista en las TI en todos sus rubros y de preferencia que dentro del organigrama de la organización se encuentre en las más altas jerarquías, nos referimos al *Chief Enterprise Officer* (CEO).

Este ejecutivo tendrá la labor de guiar, supervisar y dirigir el trabajo de un cierto grupo de personas, pero además es el encargado de entregar resultados del trabajo en equipo, a los ejecutivos de mayor rango dentro de la entidad.

Existen diferentes posiciones dentro de una organización *Chief Financial Officer* (CFO), *Chief Information Officer* (CIO) y *Chief Security Officer* (CSO), las cuales tienen a su cargo diferentes tareas. Cada uno tiene un papel muy importante en la organización y sin uno de ellos no está completa una administración.

El CSO debe comprender las necesidades globales de la organización, entender las necesidades de seguridad en TI dentro de la misma y demostrar un gran compromiso.

El CEO debe de tener claro ciertos objetivos como es el de relevar la situación de las TI dentro de la corporación, sugerir e implementar cambios dentro de la organización para que existan las tecnologías, pero además de esto tiene una importante tarea de comprometer a toda la entidad y concientizar de lo importante que son las tecnologías para el crecimiento haciendo gran hincapié que debe existir seguridad ya que esto también trae por detrás grandes riesgos que se deben tomar en cuenta y persuadir a los empleados en seguir los procedimientos de seguridad porque esto nos representa ventajas tanto para la organización como a ellos mismos.

Cuando se trata de concientizar a las personas sobre la importancia de la seguridad, se les debe hablar de una manera entendible para que ellos puedan aceptar todo lo que conlleva el utilizar TI. Ya que habrá que aplicar ciertos cambios que no les será de su agrado pero al plantearles los resultados y las mejoras que habrá ellos entenderán y los aceptarán. Para esto primero debe el ejecutivo involucrarse y comprender todo lo que va a realizar y planear las maneras en que se harán los cambios, es decir, necesita analizar todos los procedimientos.

Generalmente los ejecutivos piensan que las TI solo involucran los programas contables o el e-mail, siendo que las TI abarcan una extensa gama de herramientas indispensables; ya que pueden estar involucradas en todas las áreas, es decir, las TI comprenden todas las tecnologías basadas en computadora y comunicaciones, usadas para adquirir, almacenar, manipular y transmitir información; además que permite a las organizaciones tener un mejor manejo e integración de las necesidades de procesamiento de información en todas las áreas funcionales de ésta.

Las TI durante el transcurso del tiempo han desarrollado posibilidades para almacenar y manejar información dentro de las organizaciones, si existe este compromiso por parte del ejecutivo, de cambiar la organización y a su personal, logrará aprovechar las tecnologías y mejorar sus procesos esto lo llevará a tener ventajas competitivas y estratégicas de vital importancia en comparación con otras organizaciones. Pero para esto necesita contar con profesionistas que conozcan las nuevas TI desde el punto de vista conceptual y práctico, entienda los procesos de la organización y las áreas administrativas. Desafortunadamente hay una carencia de profesionistas involucrados en las TI lo que provoca que las organizaciones no tengan comunicación eficiente entre las áreas administrativas y las responsables de las TI.

2.1.2 Administración del riesgo y análisis

Cuando estamos planeando el manejo de la seguridad en las TI debemos tomar en cuenta como un punto importante la administración de riesgos el cual afecta al mundo financiero ya que su objetivo es minimizar los costos y evitar las pérdidas que se puedan tener. Es decir la administración de riesgos hace una relación de la seguridad con la administración financiera y proporciona herramientas para la protección de nuestros activos.

Cualquier organización que se quiere desarrollar en seguridad debe elaborar una estrategia de administración de riesgos que sea compatible con su entorno, esta estrategia necesita enfocar tanto su esfuerzo, tiempo y costo porque las necesidades que requiere para su seguridad dependen mucho del tamaño, tipo de organización, entorno y cultura.

La administración del riesgo tiene cuatro actividades específicas:

1. Determina una estrategia completa de administración de riesgos adecuada al perfil de la organización en el contexto de la política de seguridad de la organización.

2. Se realiza una selección de las contramedidas para proteger los activos de acuerdo a los resultados obtenidos por el análisis de riesgos o de un *baseline* de control
3. Se formulan las políticas de seguridad de TI tomando en cuenta las recomendaciones de seguridad.
4. Se elabora un plan de seguridad de TI que efectúe las contramedidas, basadas en las políticas de seguridad de TI aprobadas.

Las actividades anteriores las podemos ver en la Fig. 2.2 donde se ven claramente las tareas que realiza la administración para identificar y administrar los riesgos dentro de la organización.

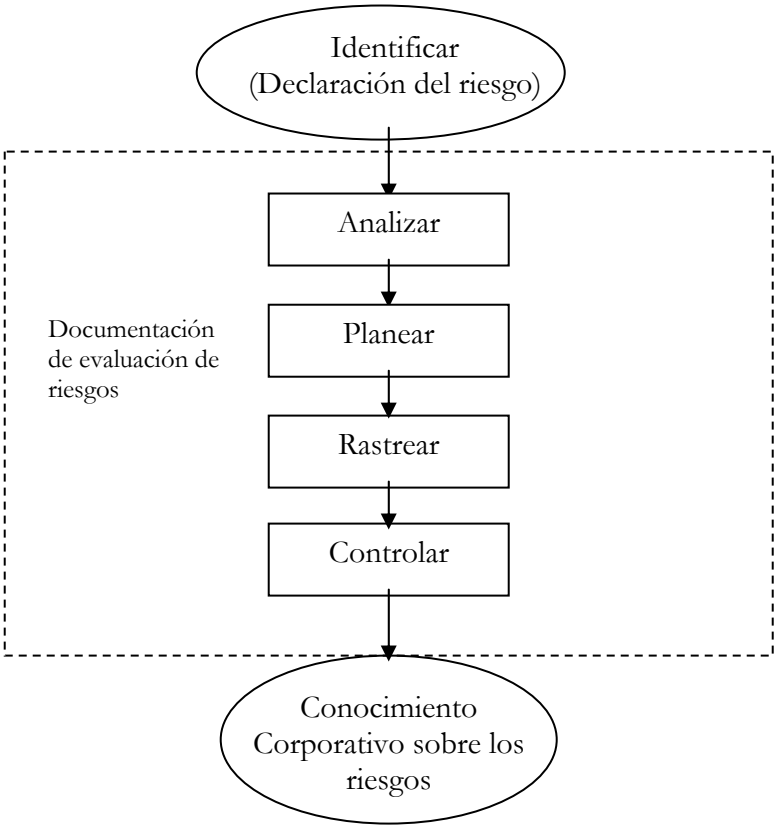


Fig. 2.2 Procesos de la Administración de riesgos

Una de las cosas que hace más difícil el análisis es calificar el beneficio de la inversión en seguridad, que su propio costo. El costo es tangible pero el beneficio es hipotético, tiene una probabilidad pero no se tiene la certeza que pueda suceder. Sin embargo aunque no se tiene una total seguridad de los beneficios se llega a un punto en donde se tiene la confianza de los beneficios que se obtendrán y esto permite a los ejecutivos medir el valor de la seguridad en función a los beneficios que proporciona.

Podemos implementar un modelo para identificar y administrar riesgos a través de todas las fases que tiene nuestra organización.

Según Suzanne Labarge, Jefe de riesgos del *Royal Bank of Canada*, "el riesgo en sí mismo no es malo. Lo que sí es malo es que el riesgo esté mal administrado, mal interpretado, mal calculado o

incomprendido". De hecho, muchos se están dando cuenta que el riesgo crea oportunidad, la oportunidad crea valor y, por último, el valor crea riqueza para los accionistas.

2.1.3 Políticas, estándares, guías básicas y procedimientos

Siempre que se encuentra una organización con el concepto de seguridad en las TI se enfrenta a un nuevo proyecto el cual ayudará planificar, coordinar e implementar el nuevo plan de seguridad de TI. Para que se tenga una plena confianza de que todo va por el buen camino se necesitan crear políticas, estándares, guías básicas y procedimientos que serán muy útiles durante el ciclo de vida que tenga cada uno. Algunos son más importantes y la falta de éstos es uno de los problemas más graves a los que se enfrenta una corporación en lo que se refiere a la protección de los activos en contra de peligros tantos externos como internos.

La aplicación de las políticas, estándares, guías básicas y procedimientos nos ayudan a proteger los activos y accionar ante eventos que pudieran suceder. El CSO (*Chief Security Officer*) es el responsable de mantener actualizadas y documentadas las políticas, estándares, guías básicas y procedimientos para asegurar la protección de los bienes informáticos de la organización.

El primer concepto que vamos a tratar son las políticas. Las **políticas** no son una descripción técnica de mecanismos de seguridad, ni leyes es mas bien una respuesta a algunas preguntas que surgen; como el que deseamos proteger y el porque de ello. Estas representan un tipo especial de reglas documentadas, las cuáles deben ser instrucciones u orientaciones claras y definitivas que ayuden a manejar y garantizar los asuntos de seguridad pero algo muy importante que hay que tener en cuenta es que éstas son obligatorias y es una de las formas en que se pueden comunicar los ejecutivos y empleados. El siguiente concepto de políticas nos deja más claro que son y para que sirven: "Las políticas son un conjunto de reglas que señalan la manera en que una organización maneja, administra, protege y asigna recursos para alcanzar el nivel de seguridad definido como objetivo."

Las políticas pueden variar dependiendo del tipo de organización, las metas, comportamientos, responsabilidades y objetivos que tenga ésta. Frecuentemente están acompañadas de normas, procedimientos e instrucciones pero si hablamos de jerarquías las políticas son superiores. Son diseñadas con el fin que se cumplan y tengan una aplicación de largo plazo las cuales guían el desarrollo de otras reglas y criterios que aborden situaciones más específicas pero algo importante es que no deben ser extensas y tienen que ser aprobadas por autoridades superiores. Si una política deja de hablar de forma general el como se maneja un problema y es mas detallado y extenso; ésta se convierte en un procedimiento.

Cabe destacar que las políticas son de jerarquía superior a los estándares, guías básicas y procedimientos aunque éstos también requieren ser respetados.

Las políticas deben especificar claramente quien es la autoridad, que debe hacer que las cosas se cumplan conforme a lo establecido, el rango de los correctivos que se realizarán y las clases de sanciones que se implementarán, aunque también debe quedar claro que cada uno de los empleados es responsable de que se cumplan las políticas.

Hoy en día existen muchas organizaciones que han creado sus propias políticas quienes tratan de llevarlas acabo capacitando a su personal, sin embargo aun tienen un problema que enfrentar ya que no han fomentado una cultura de conciencia en seguridad que ayude a identificar y reportar los problemas,

es por ello que las políticas por sí solas no constituyen una garantía, deben responder a intereses y necesidades organizacionales basadas en la visión de la corporación.

Por último cabe destacar que las políticas tienen un ciclo de vida, que se fue formando con un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la aceptaran, conseguir la aprobación, concientizar a los miembros de la importancia de las políticas, conseguir que las acaten, hacerle seguimiento, garantizar que está actualizada y quitarla cuando haya terminado su vigencia.

Los **estándares** son reglas que especifican una acción o respuesta que se debe seguir dependiendo de las situaciones que se presenten. Son orientaciones obligatorias que buscan hacer cumplir las políticas, por lo cual son diseñadas para promover la implementación de las mismas y de crear nuevas. Los estándares son un conjunto de parámetros lógicos o físicos determinados para garantizar la seguridad adecuada a las normas y procedimientos establecidos.

Una estructura organizacional soporta un enfoque armonizado de la seguridad de TI, sus necesidades son soportadas por el cumplimiento de los estándares, los cuáles pueden ser internacionales, nacionales y corporativos. Existen beneficios por usar lo estándares como son:

- Seguridad integrada
- Interoperables
- Consistentes
- Portables

Las guías básicas son una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas, es decir, son recomendaciones que deben considerarse al implementar la seguridad, aunque no son obligatorias, serán llevadas a cabo, con excepciones si es que existen argumentos documentados y aprobados para no hacerlo.

Los **procedimientos** se crean independientemente de las políticas, pero deben ser consistentes con ellas, definen específicamente cómo las políticas, estándares y guías serán implementados en una situación dada, seguirán las políticas de la organización, los estándares y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde se aplican. Además son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. También delinean los pasos que deben ser seguidos por una organización para realizar la seguridad relacionada a dicho proceso o sistema específico, requieren ser actualizados más a menudo que las políticas porque las TI cambian muy rápido. Generalmente son desarrollados, implementados y supervisados por el dueño del proceso o sistema.

No sólo existen las políticas, estándares, guías básicas y procedimientos, también no debemos de olvidar la "**mejor práctica**", la cual es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

Las políticas, estándares, guías básicas, procedimientos y mejores prácticas tienen un ciclo de vida que puede verse en diferentes fases, las cuáles varían dependiendo el concepto como se muestra en la siguiente figura.

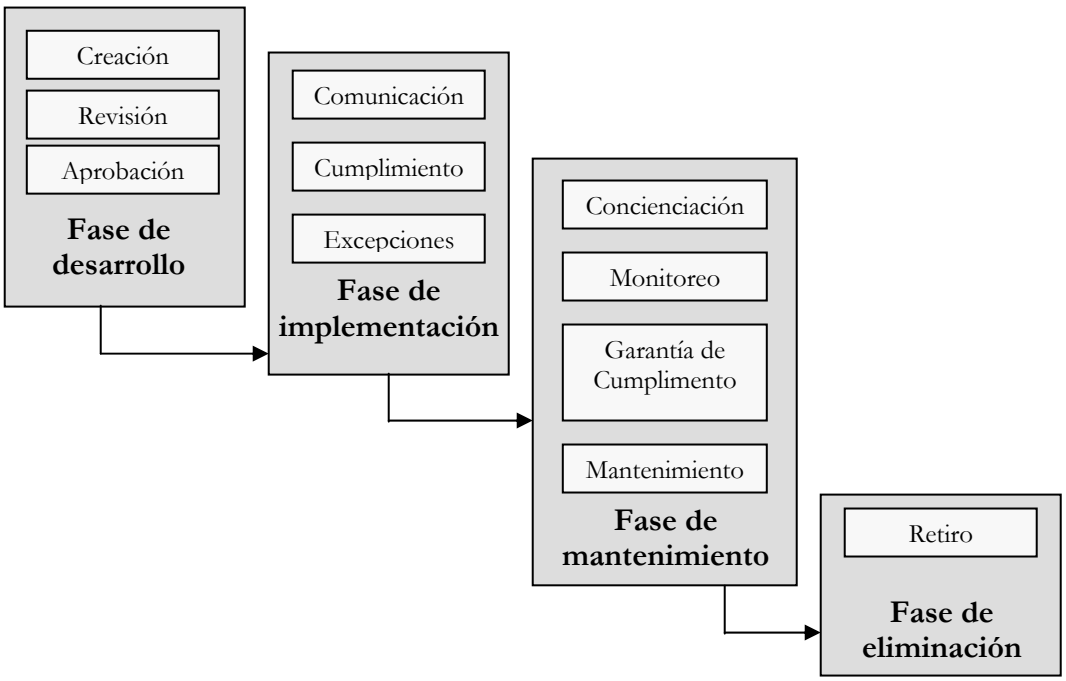


Fig. 2.3 Fases de las políticas, estándares, guías básicas, procedimientos y mejores prácticas.

2.1.4 Verificación de roles y responsabilidades

Siempre en una organización se necesita asignar responsabilidades bien definidas a cada uno de los miembros. Cuando se asignan responsabilidades se asegura que éstas tareas serán realizadas de una manera eficiente ya que cada quien tendrá su trabajo y no habrá manera de culpar a otros. No siempre se asigna las responsabilidades de la misma manera ya que depende mucho de la estructura de la entidad, así como de su tamaño y el trabajo que desempeña. La organización debe establecer una clara línea de comunicación, responsabilidad y autoridad por lo que se deben contar con las responsabilidades apropiadas.

Cuando hablamos de organizaciones pequeñas o medianas podemos tener un oficial de seguridad de TI (SO, *Security Officer)* quien asumirá las responsabilidades de seguridad pero tenemos que tener claro que si se requieren de hacer más funciones, es decir, asumir distintos roles de seguridad es necesario tener más ya que podemos caer al error de concentrar mas poder en manos de una persona el cual no sea suficiente para controlar las situaciones. Es necesario tener personas con las habilidades para identificar requerimientos, formular y participar en la elaboración de un programa de seguridad con el fin de soportar las TI. Una de las tareas que se pueden asumir es trasladar las políticas de seguridad en el programa de seguridad de TI, monitorear la implementación del programa de seguridad de TI, revisar la efectividad de las políticas y promover la concientización en materia de seguridad del personal.

Pero ¿cómo podemos definir las responsabilidades de TI? Las responsabilidades siempre serán compartidas, lo cual puede ser un riesgo grande ya que al final puede que nadie se responsabilice de nada. Para evitar esto en las TI es necesario asignar a una persona específica pero esto no quiere decir que él solo tendrá todas las responsabilidades, sino que será una persona capaz de asignar responsabilidades a otros, los cuáles darán cuentas a él para que posteriormente éste las entregue a autoridades superiores.

Cuando se verifican los roles y las responsabilidades es necesario asignar a los responsables, de tal manera que se asignan grupos de trabajo. Con los grupos se hace una separación de tareas que nos ayuda a proveer una perspectiva más amplia y diferente de asignar las responsabilidades para llegar a ser más eficientes.

Algo muy importante que tenemos que recalcar es que la seguridad de las TI es responsabilidad de todos los miembros de la organización verificando en cada uno de los niveles las acciones que deben realizarse para proteger todos los activos de la entidad.

2.1.5 Clasificación de la información

La clasificación de la información es una actividad fundamental para la administración de la seguridad pero se enfrenta a un problema común porque se desconoce el como se deben hacer las clasificaciones y por lo tanto no se hacen ya sea por negligencia o por desconocimiento.

Es importante definir la clasificación de la información la cual es un proceso que caracteriza a los diferentes tipos, estructuras y valores de la información, de esta manera las divide para que la organización pueda separarla y diferenciar los datos de libre acceso para todo el personal de aquellos datos restringidos, los cuáles pueden ser altamente confidenciales y sólo pueden ser vistos por cierto tipo de personas.

Además nos ayuda a saber con que información contamos, ya que no toda la que existe en la organización es igual de importante, por lo que cada una tiene diferente trato, alguna no es indispensable y por lo consiguiente desechable, pero existe otra que es más importante la cual debe ser guardada y protegida. Es decir se atenderá dependiendo de su mayor o menor carácter confidencial o a su criticidad.

Los objetivos de la clasificación son el reducir los riesgos y costos, identificar la información y los recursos informáticos más valiosos.

La clasificación de la información debe permitir establecer diferencias entre las medidas de seguridad a aplicar que, de forma general, atenderán a criterios de disponibilidad, integridad y confidencialidad de los datos.

Una vez clasificada la información se necesita tener un procedimiento de clasificación que nos ayude cada vez que tengamos nueva información para poderla clasificar más fácil.
La clasificación debe ser rigurosa pero a la vez ágil, ya que los esquemas complejos llegan a ser impracticables y costosos.

2.1.6 Capacitación en la seguridad informática

Cuando se implementan las TI no sólo se deben tomar en cuenta las tecnologías sino al personal ya que ellos participan y se relacionan con los activos de la entidad y por lo regular son el eslabón más débil al que se debe de reforzar haciéndoles comprender que sus acciones pueden afectar la seguridad.

El principal desafío de las organizaciones al ingresar las TI es la concientización y capacitación de todos los involucrados en cuanto a las medidas de seguridad a utilizar en las distintas áreas de la entidad. Muchas veces el personal no está consciente de la importancia y vulnerabilidad de las tecnologías y de la información que se maneja dentro de las corporaciones.

Es importante recordar que la seguridad absoluta no existe pero siempre que se busca tener una educación de la información se relacionan dos conceptos: capacitar y concientizar. Cuando hablamos de capacitar nos referimos a enseñarle al personal para que tenga la aptitud o disposición para ayudar a que la organización crezca. Mediante la capacitación se pretende que el personal se haga consciente de la importancia de las TI y la seguridad. La creación e implantación de un plan de concientización organizacional propicia que todos los niveles de su corporación cuenten con el conocimiento adecuado de la importancia de la seguridad y sus repercusiones. Podemos asegurar que la capacitación es un componente básico de cualquier estrategia de seguridad de la información, complementario a la cultura de seguridad (concientización).

Los programas de capacitación necesitan ser implementados en todos los niveles de la organización, desde la alta Gerencia hasta los usuarios más básicos, si no se acepta el programa por todos, la capacitación no tiene éxito.

Cuando se implementa la seguridad por primera vez, puede ser más eficaz si se le asignan los recursos suficientes para establecer un plan de capacitación mediante las cuales se den a conocer las políticas de seguridad de la organización, la administración, entender por completo las guías y acciones de seguridad, los estándares, procedimientos, etc. que se deberán cumplir.

Como resumen podemos decir que es necesario tener una capacitación para desarrollar una estrategia a corto y a mediano plazo, tomando en cuenta la formación de especialistas y de intermediarios tecnológicos. Pero no solo se necesita capacitación sino de una investigación la cual forma una parte primordial de un proceso en el cual la TI es el producto. Para esto se debe plantear una estrategia diferenciada de corto, mediano y largo plazo que apoye a los procesos de asimilación, adaptación, transferencia y desarrollo de TI se necesita fomentar una cultura informática tratando de impulsar una mayor toma de conciencia en cuanto a la eficiencia que brinda la correcta utilización de las TI y también impulsar un cambio profundo en la actitud y en el perfil de los empleados, para alcanzar una mayor productividad y eficiencia.

2.2 Aspectos organizacionales de la seguridad en las Tecnologías de la Información

Como acabamos de ver, la planeación abarca muchos conceptos para que una organización llegue a tener la seguridad adecuada en las Tecnologías de la Información.

A continuación se muestra un diagrama que explica todo el proceso.

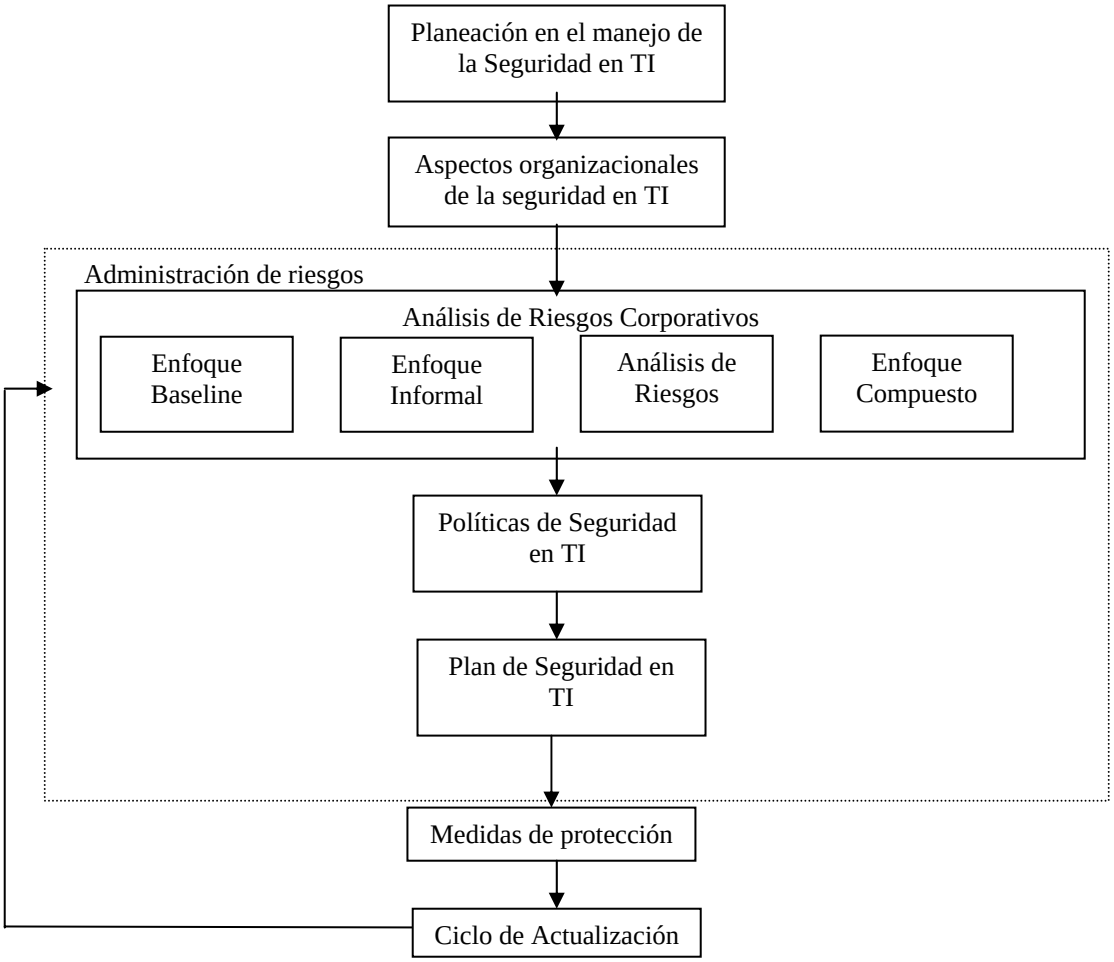


Fig. 2.4 Proceso que debe realizar una empresa para el manejo y la administración de la seguridad en las TI

Como vemos en la Fig. 2.4 todo empieza con una planeación que requiere de elementos para llevar acabo la seguridad en la organización. De esta manera se empieza a realizar un amplio estudio sobre los procesos y activos que se tienen para posteriormente clasificarlos. Obteniendo de esta manera una administración de riesgos; el cual se identifica por medio de un análisis donde se ven todos los riesgos que puede tener la corporación y de esta manera tratar de mitigarlos o afrontarlos.

Posteriormente de haber hecho un análisis es importante empezar a pensar en políticas que nos ayuden a resguardar toda la seguridad interna, pero no solo se implementan políticas sino también estándares, guías básicas y procedimientos. Es importante tener un buen plan de seguridad y medidas de protección que nos ayuden a proteger todos los activos y procesos que utiliza, aquí también tenemos la capacitación que se va a dar a los empleados y a todo el personal involucrado en las TI. Por último vemos que existe un ciclo de actualización ya que las organizaciones son dinámicas y tienen cambios continuamente por lo tanto también cambia toda la estructura de la organización. En los procesos de seguridad en TI debemos tener claro que requiere de retroalimentación en cada una de sus fases durante su ciclo de vida.

Para tener todo este ciclo en la organización es importante contar con el compromiso ejecutivo y de todo el personal involucrado, para establecer las responsabilidades y los mecanismos de capacitación en seguridad informática dependiendo del rol que tengan. Es necesario comprender a todas las tareas y estar consientes que la seguridad es importante para el crecimiento de la entidad.

2.3 Administración de riesgos corporativos

La administración de riesgo corporativo o empresarial (ERM, *Enterprise Risk Management*) es una propuesta disciplinada y estructurada que alinea la estrategia, los procesos, las personas, tecnología y conocimiento, con el propósito de evaluar y administrar las incertidumbres que enfrenta la entidad a medida que crea valor. Posee el potencial para entregar a la organización una nueva ventaja. Las organizaciones deben concientizarse que los peligros ya no sólo se encuentran en los tradicionales financieros y asegurables. Ahora deben abarcarse una serie de riesgos estratégicos, operacionales, reputación, regulatorios y de información.

La tolerancia al riesgo de las corporaciones depende de ella y su estructura por lo tanto es única, la cuál varía de acuerdo a su cultura organizacional y a factores tanto internos como externos. Un aspecto crítico que tiene es determinar que riesgos y cuantos debe tomar. "La ERM sostiene que un número definido de errores puede llegar a ser tolerado siempre y cuando el costo de protegerse de ellos no es más caro que los riesgos que ellos suponen."

Cuando ya se tiene una administración es importante contar con herramientas que nos ayuden a identificar y determinar colectivamente los riesgos a los que se enfrentan las organizaciones. Estas herramientas muchas veces ayudan a evaluar cada riesgo con probabilidades que determinan si el riesgo ocurre y cual sería su magnitud. También pueden ayudar a identificar a los "dueños" de riesgos, es decir, aquellos a quienes la organización les asigna la responsabilidad y autoridad para la administración de los riesgos.

Las herramientas se dividen en dos clases:

- Las herramientas de clasificación las cuáles ayudan a la organización a agrupar y darle prioridad o jerarquía a los riesgos dentro de la entidad. De esta manera asegura que se han encontrado y clasificado todos los riesgos de la organización.
- Las herramientas de cuantificación financiera permiten entender el impacto potencial de riesgos. En esta parte encontramos modelos que nos permiten evaluar riesgos en áreas financieras.

La dirección que lleva la administración de riesgos puede ser centralizada a nivel corporativo o descentralizada entre divisiones o procesos dependiendo de los riesgos.

La administración de riesgo centralizado se enfoca en los riesgos que afectan los objetivos y estrategias corporativas, afectando todas las funciones o procesos de la corporación (por ejemplo, la reputación).

La administración de riesgo descentralizado, atiende riesgos que sólo afectan a un proceso, son mejor administrados ya que están presentes en un proceso en particular, sin embargo, si pueden afectar la habilidad de la entidad en la implementación de sus estrategias.

Existe una categoría de riesgos dentro de la organización la cual podemos verla en la siguiente figura:

Fig. 2.5 Riesgos en la Organización

Es necesario crear un programa de trabajo ERM y asignar ejecutivos llamados (CRO, *Chief Risk Officer*), quienes serán los responsables de desarrollar y manejar las estrategias de la administración de riesgos, no importando si es de forma centralizada o descentralizada. La evaluación de los riesgos les permiten a los CRO´s percibir los impactos y saberlos manejar de tal manera que favorezca a la corporación tanto en tiempo como en inversión.

Por ultimo la ERM si es integrada puede conducir a cambios impresionantes en la organización, para que esto tenga éxito se necesita del apoyo del Gerente General y el Director ya que su principal tarea es difundirla en toda la organización. Además que la administración de riesgo puede ser una ventaja estratégica competitiva si es utilizada para identificar acciones que mejoren el desempeño y optimicen. Bien utilizada la ERM se convierte en un instrumento valioso en la organización que ayuda a redireccionar su enfoque perfeccionando la toma de decisiones, en lugar de responder a las crisis.

De manera general podemos decir que la ERM es:

- Es un proceso continuo que fluye por toda la entidad.
- Es realizado por su personal en todos los niveles de la organización.
- Se aplica en el establecimiento de la estrategia.
- Se aplica en toda la entidad, en cada nivel y unidad, e incluye adoptar una perspectiva del portafolio de riesgo en los niveles de la entidad.
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del riesgo aceptado.
- Es capaz de proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad.

- Está orientada al logro de objetivos dentro de unas categorías definidas, aunque susceptibles de traslaparse.

2.3.1 Análisis de riesgos corporativos

Antes de hablar de análisis de riesgos, hay que recordar que los riesgos son la probabilidad de que una amenaza aproveche las vulnerabilidades o la ausencia de controles para impactar en cualquiera de las características de la seguridad como son la disponibilidad, confidencialidad, integridad, etc.

El nivel de riesgo al que está sometido una organización no se puede erradicar hasta su totalidad. Pero se puede buscar un equilibrio entre el nivel de recursos y mecanismos los cuales minimizan los riesgos y un cierto nivel de confianza que puede considerarse como un riesgo aceptable.

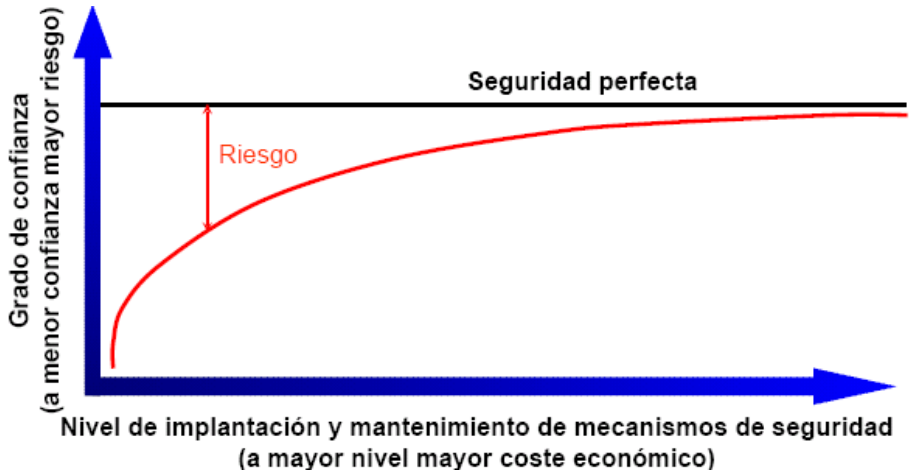


Fig. 2.6 Nivel del riesgo en una organización

El análisis de riesgos es el punto de inicio que se debe cumplir en cualquier procedimiento de la administración de la seguridad en TI basándose en estándares de seguridad evaluando las vulnerabilidades potenciales de seguridad de los procesos de la organización y de esta manera definir los planes de mitigación.

Es un procedimiento de ayuda a la decisión. Se encarga de estudiar los activos, posteriormente se identifican las amenazas que están en contra de los activos, las vulnerabilidades, impactos y riesgos que existan, su objetivo principal es proporcionar evidencias racionales que permita tomar decisiones sobre la seguridad y de esa manera cumplir con su misión, sus resultados constituyen una guía para tomar decisiones sobre si es necesario implantar nuevos mecanismos de seguridad y que controles o procesos de seguridad serán los más adecuados.

Cuando se hace un análisis se seleccionan e implementan las medidas de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Aunque no existe algo seguro porque sabemos perfectamente que los incidentes no tienen un modelo a seguir ni se repiten de la misma manera y por lo tanto no afectan a las corporaciones de la misma forma.

Durante el análisis, la organización toma las medidas dependiendo de los costes de la implantación de controles que reduzcan los riesgos vs. Costes derivados de las consecuencias de la materialización de estos riesgos. Los pasos que se siguen son:

- Mitigar el riesgo: A través de la creación y mantenimiento de controles de seguridad se minimizan los riesgos y se mantienen en un nivel aceptable (lo cual implica inversiones económicas).
- Asumir: La organización necesita tomar ciertos riesgos a los que esta expuesta ya que las consecuencias acarrean un coste económico y estratégico menor que el coste que sería necesario aportar para reducir dichos riesgos.

El proceso de análisis de riesgos puede caer en errores comunes, como son: dificultad excesiva para identificar amenazas, vulnerabilidades y sus consecuencias, un pobre entendimiento de las amenazas y sus capacidades, habituarse a una situación existente, ignorar las defensas exitosas, malinterpretar datos estadísticos, ignorar el problema del tiempo, subestimar la interdependencia y la complejidad del análisis, tener un enfoque netamente reactivo, generar una confianza excesiva al interior, o tener un foco inadecuado sobre los riesgos de negocio de alto nivel.

Existen dos tipos de análisis:

Cuantitativa: Este análisis es el más complejo ya que necesita hacer cálculos complejos o datos difíciles de estimar. Se basa en la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas si es el caso.

Cualitativa: Es más sencillo e intuitivo que el anterior, en este análisis no se utilizan las probabilidades exactas por el contrario utilizan una estimación de pérdidas potenciales. Para esto se relacionan cuatro elementos principales: las amenazas, las vulnerabilidades, el impacto asociado a una amenaza y los controles. Con estos elementos se obtiene el cualitativo del nivel de riesgo asociado a un activo de la entidad, viéndolo como una probabilidad de que la amenaza se materialice sobre uno de los activos y produzca un impacto.

Existen diversos enfoques de gestión del riesgo como son: enfoque de línea base, enfoque informal, detallado y combinado. Los cuales se explicarán posteriormente.

2.3.1.1 Enfoque de línea base o *baseline*

Los enfoques de línea base o *baseline* son soluciones genéricas que se basan en buenas prácticas, las cuales se adaptan a recomendaciones de la industria y se aplican en toda la infraestructura. Podemos decir que es una medición de los indicadores antes que se inicie un proyecto.

Como en todos los métodos existen ventajas y desventajas; las ventajas de este enfoque es que no requieren de grandes recursos para realizar un análisis de riesgos detallado y el tiempo y esfuerzo invertido para seleccionar la solución es reducido, regularmente no se requiere de muchos esfuerzos para adaptar un *baseline* similar de seguridad a distintos sistemas. También es importante mencionar las desventajas como: si el nivel del *baseline* es muy alto, éste será muy caro o muy restrictivo para algunos sistemas, y por el contrario si el nivel del *baseline* es demasiado bajo, muy probablemente la seguridad será poco efectiva para algunos sistemas y existen algunas dificultades en administrar los cambios relevantes de seguridad.

2.3.1.2 Enfoque informal

La segunda opción es realizar un análisis de riesgos en los sistemas de manera informal y pragmático. No se basa en una metodología estructurada, sin embargo explota el conocimiento y experiencia de las personas ya sea porque éstas se encuentran dentro de la organización o bien gente especializada que se dedica a consultoría.

Las ventajas que se pueden encontrar es que no se requieren de habilidades especiales para llevar a cabo un análisis informal, se lleva de manera más rápida que un análisis formal. Pero cuando no se tiene un análisis formal se carece de un enfoque estructurado y la probabilidad de errar sobre algunos riesgos es realmente alta. Los resultados pueden ser influenciados por visiones subjetivas o por prejuicios del analista y regularmente la selección de las soluciones de seguridad no se encuentran lo suficientemente justificadas.

2.3.1.3 Análisis de riesgo detallado

El análisis de riesgo detallado lo primero que realiza es verificar y valorar los activos identificando los riesgos y sus vulnerabilidades. Posteriormente los niveles de seguridad apropiados son identificados dependiendo de las necesidades del sistema, se seleccionan y adoptan las soluciones de seguridad para la protección de los activos, llevando los riesgos a niveles aceptables. La administración de los cambios en la seguridad son beneficiados por obtener información adicional de un análisis de riesgos. Un análisis de riesgos puede ser un proceso que consuma recursos, y de esta forma se requiere establecer fronteras y una constante atención por parte de la administración.

Una de las principales desventajas de este análisis es el tiempo, ya que puede ser algo considerable además del esfuerzo y una experiencia grande para obtener resultados.

2.3.1.4 Enfoque combinado

Por último el enfoque combinado, como su nombre lo dice es una combinación del *baseline* y análisis de riesgo detallado explicados anteriormente. Se obtiene un mejor enfoque ya que proporciona un buen balance entre minimizar el tiempo y esfuerzo invertido en identificar soluciones, mientras asegura que todos los sistemas serán protegidos de forma apropiada. Para esto se necesitan identificar las operaciones que se consideran críticas que representan un gran riesgo para la organización, esto a través de un análisis de riesgos de alto nivel, basándose en estos resultados, los sistemas son categorizados para realizar un análisis de riesgos a detalle para lograr una apropiada solución de seguridad e integración de *baselines*.

Ventajas:

- Un enfoque de alto nivel para obtener la información necesaria acerca de los recursos significativos y una alta probabilidad de obtener un programa de administración de riesgos aceptable.
- Construcción inmediata de una estrategia de seguridad, que puede ser guía para la planeación.
- Los recursos pueden ser aplicados donde realmente benefician más y sobre sistemas que probablemente representen un riesgo alto para la organización.

Desventajas:

- Si el análisis de riesgos de alto nivel genera resultados inadecuados, algunos sistemas importantes no serán identificados. Esto es improbable si el resultado del análisis de alto nivel es verificado apropiadamente.

2.3.2 Políticas de seguridad para las Tecnologías de la Información

Las organizaciones se han dado cuenta que cuando se consideran las TI y su seguridad existe una transformación y cambios en los procesos administrativos en la forma de innovar y administrar, alcanzando con plenitud sus potenciales. Y saben que gran parte de su éxito está ligado a la definición de las políticas en TI y su administración.

Hemos explicado anteriormente que las políticas son el canal para que tengan una comunicación los miembros con los activos de una manera correcta. Son las reglas para lograr los objetivos de la corporación, las cuáles son definidas específicamente para cada área. Para que exista la seguridad en TI es necesario tener bien claro los objetivos, estrategias y políticas.

Como en las otras políticas se desarrollan documentos y directrices que ayudan al uso adecuado de las tecnologías y dan recomendaciones para obtener un mejor provecho de las ventajas, además de evitar el mal uso de ellas, lo cual podría ocasionar graves problemas dentro de la corporación.

Podemos decir que las políticas de seguridad en TI surgen como herramientas organizacionales para concientizar de alguna manera a los miembros de la importancia que tienen las TI.

Así como las otras políticas el proponer o identificar las políticas de seguridad en TI necesitan de un alto compromiso, la habilidad para detectar las fallas y debilidades, para de esa manera crear las políticas que ayuden a protegerlas. Esto se hace a través de un análisis de riesgos en donde se valoran todos los activos y se comunican todos los riesgos y beneficios al implementar las políticas. También es importante especificar quien es la autoridad para tomar las decisiones pues de ésta manera se salvaguardan los activos críticos de la organización. Como se ha explicado anteriormente se desarrolla un proceso de monitoreo periódico de las directrices que permitan verificar que todo se está realizando conforme se tenía previsto, además de encontrar las mejoras en las políticas y actualizarlas.

En la Fig. 2.7 podemos observar la relación que existe entre cada una de las políticas, teniendo en cuenta que pueden cambiar dependiendo del tamaño de la organización.

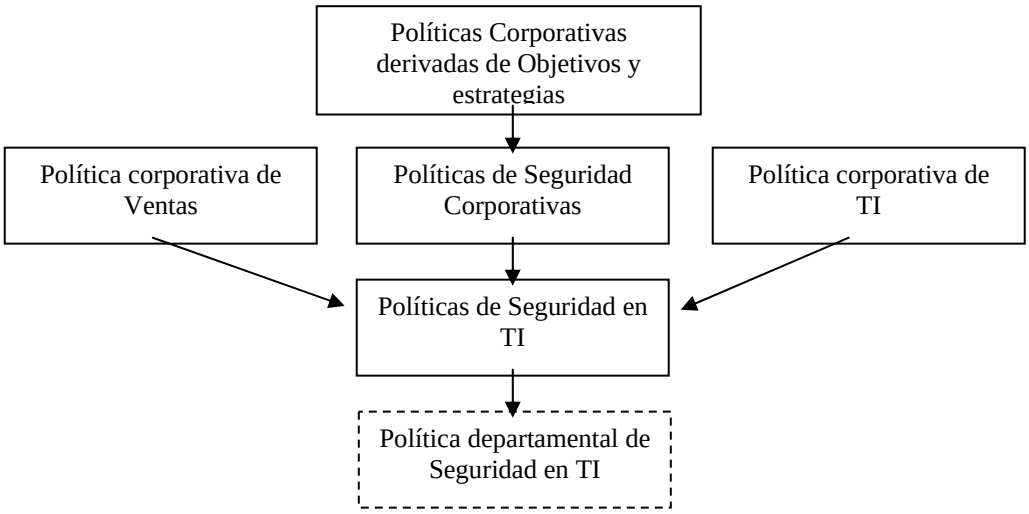


Fig. 2.7 Tipos de Políticas dentro de una organización

2.3.3 Plan de seguridad informático

Siempre que se empieza con la seguridad informática se requiere de un análisis del trabajo, dependiendo de eso se crean documentos llamados plan de seguridad de TI en donde se explican las acciones que deben realizarse a cabo para implementar la seguridad en los activos. En este plan se encuentran las acciones principales que se llevarán a cabo a corto, mediano y largo plazo, así como su costo de inversión y tiempo de implementación:

En el plan de seguridad de TI podemos incluir:

- Desarrollo de arquitectura de seguridad.
- Revisiones de los sistemas de TI para verificar el apego a los objetivos de seguridad.
- Identificación de las soluciones de seguridad correspondientes a la valoración del riesgo.
- Un análisis de los actuales niveles de confidencialidad que integran las soluciones de seguridad.
- Un resumen de los riesgos residuales en el contexto del sistema o de la aplicación.
- La identificación y definición de las acciones con sus respectivas prioridades a ser implementadas.
- Un detallado plan de trabajo para la implementación de soluciones, incluyendo prioridades, presupuestos y calendarización.
- Administración de proyectos, incluyendo:
    - Los recursos comprometidos.
    - Asignación de responsabilidades.

- Definición de procedimientos para reportar el progreso.

- Capacitación y concientización de seguridad para el staff y usuarios terminales.
- Requerimientos para el desarrollo y administración de sistemas.

Otra cosa importante que está adjunta al plan son los procedimientos, condiciones y acciones para validar cada uno de los puntos mencionados anteriormente.

2.3.4 Medidas de protección como soluciones de seguridad

Existen diferentes tipos de soluciones de seguridad, comenzando desde las que tienen un objetivo preventivo, de monitoreo, de detección o corrección de incidentes indeseados, hasta las orientadas a la recuperación. Las herramientas preventivas pueden disuadir actividades indeseables fortaleciendo la concientización sobre seguridad. Las principales áreas, donde las soluciones de seguridad son aplicadas se muestran a continuación:

- Hardware (alarmas, video, entre otras).
- Software (firmas electrónicas, control de accesos, antivirus, entre otras).
- Comunicaciones (firewall, cifrado de información, entre otras).
- Entorno físico (biometría, protecciones, entre otras).
- Personal (capacitación y concientización del personal, procedimiento, etc.).
- Administrativas (autorización, control de licencias, entre otras).

Las soluciones de seguridad no son independientes unas de otras y con frecuencia trabajan de forma combinada. El proceso de selección debe considerar esta interdependencia, durante la selección de soluciones debe verificarse que no existan brechas entre estas, porque pueden generar amenazas accidentales.

Muchas organizaciones tratan de resolver sus problemas de seguridad comprando productos (de hardware, software, o servicios) y creen que con eso resuelven su problema pero se necesita de un amplio estudio y una infraestructura organizativa adecuada para la seguridad informática porque todas las corporaciones son diferentes y requieren de diferentes herramientas.

Algunas medidas de protección son: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos. Se requiere tener un mantenimiento de medidas de protección, que aseguren la continuidad y efectividad de operaciones, así como la verificación del alineamiento de las medidas de protección con las políticas y planes de seguridad aprobados.

Las medidas de protección se pueden clasificar de dos maneras:

- Las que reducen la vulnerabilidad; las cuáles buscan reducir la probabilidad de incidentes, protegiendo a la organización de amenazas. Estas son llamadas medidas preventivas donde encontramos la adquisición de componentes de filtrado (Firewall, *Proxies*, Anti-Virus) y proyectos orientados a la identificación y minimización de amenazas (Diseño seguro de red de datos, VPN, Diagnósticos de seguridad, Estudios de Penetración).

- Las que minimizan el impacto; están orientadas a la detección temprana del evento y su respuesta oportuna, tales como medidas paliativas (discos RAID, copias de seguridad y enlaces de comunicación redundantes), y sistemas de monitoreo (*Event Management*, IDS: *Intruder Detection System*, entre otros).

El objetivo que se tiene es proteger a la organización; por lo que se toman medidas para enfrentar las amenazas informáticas; una de las primeras que se implementa es la seguridad física que son medidas de protección externas, son las primeras por la ocurrencia de una catástrofe la cual tendría pérdidas que serían completas. Normalmente, se implementan mediante dispositivos eléctricos, electrónicos, etcétera.

2.3.4.1 Hardware

El hardware es el elemento más caro de todo el sistema informático, por lo tanto las medidas ayudan a asegurar su integridad, existiendo una gran disponibilidad de soluciones efectivas y accesibles que pueden ser implementadas, sin embargo las organizaciones eligen las herramientas que utilizarán para su seguridad, de esta manera podemos mencionar diferentes ejemplos de herramientas básicas como son los firewalls, motores antivirus, dispositivos o aplicaciones para detección y prevención de ataques de intrusos. Hay también soluciones más sofisticadas y poderosas, como son los dispositivos integrados de seguridad y las metodologías de capas múltiples, que cubren a las máquinas cliente, los servidores, el *gateway* y todo lo que haya entre ellos.

A pesar de todas las medidas de prevención que se tomen, ningún dispositivo de cómputo conectado a una red puede estar cien por ciento seguro, es por eso que la mejor seguridad es la que se extiende en múltiples capas de defensa.

Puesto que los sistemas informáticos suelen estar cercanos al usuario final o al mismo administrador, están expuestos a un mayor peligro de uso malintencionado. Debido a esto no se puede confiar plenamente en el cumplimiento de políticas o normativas de uso de las máquinas y estas están expuestas a intrusos ajenos al personal, que hayan logrado superar los controles de acceso de niveles superiores, por esta razón se deben configurar las máquinas y dispositivos de red de manera que sea complicado realizar manipulaciones sobre ellos, tanto a nivel físico como a nivel informático siempre que sea posible.

2.3.4.2 Software

El software es otro de los elementos clave en la parte de prevención. Se debería tener en cuenta la siguiente lista de comprobaciones:

1. Tener el software imprescindible para el funcionamiento de la actividad. Tener controlado al personal en cuanto a la instalación de software, es una medida que va implícita. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse software pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.

2. Disponer del software de seguridad adecuado. Cada actividad forma de trabajo métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones organizacionales.

3. Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.

4. Asegurar licencias. Determinado software imponen métodos de instalación, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.

5. Buscar alternativas más seguras. Existe software que es famoso por la cantidad de agujeros de seguridad que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

2.3.4.3 Comunicaciones

La mejor manera de proteger las comunicaciones es implementando firewalls y necesariamente algunas formas de cifrado para que tengan seguridad. En esta parte se requiere administrar las operaciones, integrando los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

Cuando hablamos de Internet, redes locales, aplicaciones compartidas y el comercio electrónico es necesario mencionar los firewall (cortafuegos). Estos componentes de software, hardware, o combinación de ellos, son fundamentales para salvaguardar la integridad de la información en una sociedad cada vez más dependiente de las redes de datos.

Otro elemento que debemos mencionar son las VPN´s (Virtual Private Network) las cuales son redes privadas virtuales de datos que funcionan sobre una infraestructura de red pública de telecomunicaciones en la cual también se implementa la seguridad a un nivel muy alto, además de tener la ventaja de ahorros en costos, permitiendo una escalabilidad ágil para incorporar nuevos puntos a la red en forma eficiente y económica y la compatibilidad con las nuevas tecnologías de comunicaciones. En esta red se cifran los datos antes de ser enviados a través de la red pública y se descifran cuando llegan al usuario final.

Por último cuando hablamos de comunicaciones es importante tomar en cuenta la seguridad en la transmisión de los datos. Para esto se utilizan mecanismos de seguridad capaces de cifrar la información de tal manera que solo las personas autorizadas puedan verla. El cifrado garantiza que la información no es inteligible para personas, entidades o procesos no autorizados. La manera de cifrar consiste en transformar un texto claro a un texto cifrado mediante un proceso, por medio de una información secreta o clave de cifrado. Existen dos maneras de cifrar; una de ellas se llama criptografía simétrica la cual se emplea cuando se tiene la misma clave para cifrar y descifrar en cambio si se utilizan diferentes claves se llama asimétrica, de esta manera para poder cifrar se necesita tener una clave pública conocida por todos y una clave privada la cual se mantiene secreta para poder descifrar los textos.

2.3.4.4 Entorno físico

Las medidas de protección en el entorno físico, lo relacionamos con la forma en que se resguardan las herramientas. De tal manera que se identifican los perímetros de seguridad para establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas. Es muy

importante sensibilizar a los empleados y usuarios sobre los riesgos obtenidos, si no se tiene una seguridad física, cualquier persona puede tener acceso físico por lo que el resto de las medidas de seguridad implantadas son inútiles.

Unos ejemplos de prevención podrían ser: los analizadores de retina iris, tarjetas inteligentes, videocámaras, vigilantes, etc. Una manera fácil y barata de prevenir daños es controlando el acceso a las salas y cerrándolas con llave resguardando de esta manera los equipos informáticos.

Para la detección de accesos se utilizan medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas. Si se tiene un control del acceso a las computadoras hace más difícil el robo o daño de los datos o el equipo.

2.3.4.5 Personal

Finalmente este punto lo hemos tocado anteriormente el componente que frecuentemente no permite que se realicen las soluciones de seguridad es el factor humano, independientemente del nivel de conocimiento o las intenciones que se tengan el usuario puede poner en riesgo la seguridad. Las medidas de prevención que se pueden realizar en el personal son a través de la capacitación y concientización de los miembros, para que lleven a cabo los procedimientos y finalmente se tenga seguridad.

Una de las maneras para reducir la vulnerabilidad generada por el comportamiento de los usuarios y personal es la capacitación, que permita entender con detalle qué hacer, cuándo y cómo. Finalmente es importante darnos cuenta que la seguridad del personal no es la óptica de protección civil, sino la manera de proporcionar controles a las acciones del personal que opera con los activos de la organización. Su principal objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana.

2.3.4.6 Administrativas

Por ultimo tenemos las medidas de prevención administrativas. Un ejemplo son la autorización y control de las licencias del software que se utiliza. Las licencias son la autorización o permiso concedido por el autor del software al usuario, para utilizar éste en una forma determinada.

Es muy importante tener un control sobre los programas que se tienen, ya que pueden ocasionar muchos problemas, uno de ellos podría ser que se tengan programas innecesarios que estén gastando recursos, o bien sean programas no autorizados los cuáles pueden ocasionar problemas legales a la organización.

2.4 Inversión en la seguridad para Tecnologías de la Información

Cómo lo hemos estado planteando anteriormente cuando se quiere tener una administración de la seguridad de la información es importante contar con herramientas que nos ayuden a desarrollar planes efectivos sobre la estrategia de seguridad. Pero siempre se cuestionan ¿cuánto se tiene que asignar de recursos (tiempo y dinero) para poder invertir en la seguridad?

Cualquier actividad en la organización relacionada a la gestión de la seguridad requiere de una inversión tanto económica como humana, y necesita ser rentable. Cuando se habla de la inversión de seguridad ésta debe servir de tal manera que la organización obtenga un beneficio mayor a la inversión inicial

aunque resulta difícil medir el beneficio que se obtuvo, ya que cuando se invierte en seguridad un punto importante que hay que ver es que las amenazas no se eliminan sino que se mitigan; es por eso que cuando se invierte en la seguridad significa que se conseguirá el mayor beneficio posible.

Cuando se explotan técnicas cuantitativas su principal propósito es producir resultados para el desarrollo de estrategias, impactando tanto la toma de decisión como la implementación tecnológica. La inversión en la seguridad, algunas veces no se sabe como evaluarla, pero existen un modelos como el (ROSI*, Return on Security Investment*) para calcular el valor financiero de la inversión en seguridad, entre otros.

De acuerdo a un informe emitido por la *Internacional Data Corporation* (IDC), actualmente el sector de TI cuenta con 1.100.000 organizaciones que mantienen 11 millones de puestos de trabajo de TI, con altas remuneraciones, que generan $900.000 millones en impuestos y $1,7 billones al año para la economía global. Podemos decir que en el mundo entero el sector de TI es un motor para el crecimiento económico, se ha demostrado que las inversiones de TI aumentan el Producto Interno Bruto (PIB) y la productividad del país, si estos son bien utilizados. Un estudio de investigación realizado por NASSCOM, la Asociación Nacional de Compañías de Software y Servicios de la India (*National Association of Software and Service Companies*), se comprobó que un aumento del 10% en las inversiones de capital de TI eleva el PIB en 3,6% y que un aumento del 10% en las horas trabajadas pueden aumentar el PIB hasta el 4%. Por el contrario, en las economías que cuentan con menos capital de TI (las economías que invierten menos en TI), un aumento del 10% en capital de TI produce sólo un aumento del 1,6% en el PIB y un aumento del 10% en las horas trabajadas no tiene un impacto significativo en el PIB. La inversión promedio en TI de las economías con mayor inversión en TI fue del 38,7% en 2003 y se espera que aumente al 40,2% en 2007. Por el contrario, la participación anual promedio del software en la inversión en TI de las economías con menor inversión en TI fue sólo del 17,2% en 2003, y se espera que a penas alcance el 17,7% en 2007. Es por eso que se llega a la conclusión que si se tiene mas inversión de TI en las organizaciones mayor será el beneficio que se obtendrá tanto en la economía como en la productividad; ya que se reduce el tiempo de algunos procesos y por lo tanto sus costos.

Siempre que se desea implementar algo nuevo en las organizaciones, relacionado a las TI, se cuestiona lo siguiente: ¿cuánto se tiene que invertir? y si ¿será bueno? Para esto se necesita de un trabajo en equipo de los CIO (*Chief Information Officer*) y los directivos para que se evalúen las iniciativas de inversión en TI para asegurar que haya retornos; ya que muchas veces cada uno de los proyectos de TI son aislados lo que termina en iniciativas vacías y acarrean grandes problemas. En la actualidad las entidades valoran más las decisiones individualmente, aisladas unas de otras, y pierden la oportunidad de aumentar los beneficios mediante la introducción de una solución más compleja que resuelva varios problemas actuales y futuros de una vez. Para determinar el valor de una inversión en TI se requiere considerar el riesgo, los tiempos y el contexto, de esa manera verificar, dónde, cuándo y cuánto invertir.

Al tomar decisiones de seguridad relacionada con TI, algunas organizaciones se basan en análisis razonados en la proyección de lo que podría llegar a suceder en el peor de los casos, cuando adoptan este sistema se apoyan en la hipótesis de eventos catastróficos potencialmente devastadores, y justifican sus inversiones alegando el impacto económico que tendría un absoluto cataclismo a nivel de seguridad. Pero lo hechos no llegarán en la mayoría de los casos a demostrar la justificación del gasto y por lo tanto la directiva puede creer que sólo se esta gastando dinero. El impacto que puede generar un problema de seguridad TI puede ser grande, es por eso que cualquier tipo de riesgo se valora para tomar en cuanta el tamaño de la inversión para mitigar los riesgos.

Aunque es bien sabido que no siempre se toma en cuenta todos los mecanismos de protección desde un principio, por lo regular se empieza con algunas herramientas que posteriormente hacen necesarias

otras, lo cual genera un mecanismo de inversión incremental para protegerse contra una falla total de seguridad.

Los beneficios que se obtienen de las inversiones en las TI muchas veces no son cuantificables ya que los resultados positivos (como es la productividad, la imagen, la actitud, satisfacción del personal, etc.) que arrojan son difíciles de estimar en cuestión de dinero que por lo regular son pasados por alto pero realmente significativos. Otro punto difícil de calcular pero importante es el medir los éxitos y los fracasos reales para verificar de esa manera que se están cumpliendo las expectativas de las inversiones de las TI. Es importante considerar el tiempo de los proyectos ya que se puede tener una inversión que en poco tiempo quede obsoleto y por lo tanto en vez de retornar la inversión será una pérdida.

Existen métodos para ayudar en la toma de decisiones. Uno de los mas sencillos es el Retorno de la Inversión (ROI) el cual es utilizado para comparar diferentes alternativas de inversiones y conocer lo acertado de una inversión, algunas organizaciones lo usan como un factor para tomar decisiones e invertir en el desarrollo de una nueva tecnología o entender una ya existente; aunque para algunos es demasiado simple y lo consideran poco fiable por lo que se inclinan mas por el cálculo del valor neto de una determinada inversión en un momento dado (NPV-*Net Present Value*) ya que refiere al valor de un proyecto durante todo su ciclo de vida.

ROI es la relación que permite determinar la rentabilidad de todos los capitales invertidos. Su medición resulta problemática, por la entrada en juego de diversos factores, cuya asociación a términos financieros es compleja, y los cuales varían dependiendo de las organizaciones. Uno de los principales en la actualidad es el cambio tecnológico, el carácter único de cada proyecto lleva a diferentes interpretaciones del ROI, la ausencia de una gestión financiera rígida de los proyectos y factores intangibles como satisfacción de usuarios y mejoras de comunicación.

La fórmula de ROI es el retorno esperado menos el costo de la inversión entre el costo de la inversión.

$$\frac{Retorno\_Esperado - Costo\_Inversión}{Costo\_Inversión}$$

Es importante tomar en cuenta que ROI es utilizado más en visiones a corto plazo pero cuando queremos analizar a largo plazo en términos financieros es mejor utilizar el Valor actual neto (NPV, *Net Present Value*). Es una cantidad que expresa cuánto valor se logrará de efectuar una inversión en un proyecto específico. Se realiza ajustando o descontando todos los procesos de un cierto plazo hasta el momento cero o inicial de la inversión. Si el método del NPV resulta en una cantidad positiva quiere decir que se puede implementar en la organización ya que resultará una buena inversión.

El NPV es la diferencia entre la suma de los flujos de fondos descontados que se esperan conseguir de la inversión (proyecto), y la cantidad que se invierte inicialmente. Uno de los elementos más importantes cuando se calcula NPV es el "factor" el cual es el rango estimado de retorno que permite colocar el efectivo en otras formas de inversión. Compara el comportamiento de las distintas soluciones en base al tiempo.

La fórmula que nos permite calcular el Valor Presente Neto es:

$$\sum_{n=0}^{N} \frac{I_n - E_n}{(1+i)^n}$$

I_n representa los ingresos y E_n representa los egresos y se toma como valor negativo ya que representa los desembolsos de dinero. N es el número de períodos considerado (el primer período lleva el número 0, no el 1). El valor I_n - E_n indica los flujos de caja estimados de cada período. El tipo de interés es i.

Aunque se considera un método mejor que el ROI y es más utilizada para tomar decisiones de inversión cabe destacar que también tiene sus limitaciones; ya que no toma en cuenta la flexibilidad e incertidumbre después de la decisión sobre el proyecto y no analiza los beneficios intangibles.

Existe otra más; la Tasa Interna de Retorno (IRR, Internal Rate of Return) el cual es el tipo de descuento que entrega un valor actual neto de cero para una serie de flujos de fondos futuros. Al igual que el NPV Y ROI, el IRR es utilizado para decidir qué inversiones deben realizarse y cuáles no.

2.4.1 Retorno de inversión de la seguridad

Cuando nos referimos al retorno de inversión de la seguridad, estamos hablando de la recuperación o reembolso de la inversión que se realizó en las TI. Si bien podemos decir que es un cálculo de cuándo, cómo y dónde la inversión que se realizó será recuperada a través de los beneficios que aporte. El CIO debe elaborar un informe donde de a conocer costos y beneficios de los proyectos, el balance final hablará del retorno de inversión. Cuando ya se realizaron los cálculos para el retorno de la inversión ya sea con ROI, NPV o IRR y se ha proporcionado un mecanismo de medición del riesgo el siguiente paso es esperar a que se cumpla el plazo, pero desafortunadamente algunas organizaciones no están dispuestas a esperar y quieren recuperar de inmediato la inversión.

Debemos obtener algunos indicadores económicos para evaluar las inversiones, posteriormente buscar el método de análisis de riesgos que mas se ajuste a nuestras expectativas y adaptarlo a la organización. Hemos estado hablando de ROI pero en cuestión de seguridad de la Información su derivado es ROSI (Return on Security Investment) conocido como el retorno sobre la inversión de seguridad, es el ahorro en incidentes de seguridad, de esta manera se aumenta la inversión o se consigue un incremento significativo reubicando la inversión. Es decir se da una valoración financiera de algunos riesgos que se quieren disminuir sin embargo el problema de ROSI es que la mayoría de los beneficios no se reflejan directamente porque se dedica a la reducción de pérdidas esperadas por fallas, errores o ataques, los cuáles ya no serán realizados por tener la seguridad.

ROSI está enfocado hacia beneficios monetarios y no contempla los beneficios secundarios su estimación considera tanto beneficios cuantitativos como cualitativos.

2.4.2 Factores del retorno de inversión de la seguridad

Tener los factores en la ecuación de ROSI y calcularlos no es una tarea sencilla, en estos momentos no existe un modelo estándar para calcular el riesgo financiero asociado a un incidente de seguridad, ni un método estándar para determinar la mitigación del riesgo dando una solución efectiva de seguridad. Existen métodos que toman en cuenta el hardware y software, mientras otros integran costos internos.

La mitigación es un valor muy difícil de calcular, desarrollar métricas internas que definan este valor es lo mas adecuado. Aunque no exista un modelo estándar para calcular los parámetros de ROSI, el

resultado final puede variar, pero si los cálculos son consistentes al interior de la organización, estos sirven.

Cuando calculamos el ROSI se deben producir resultados repetibles y consistentes, si esto sucede se puede considerar una herramienta poderosa para realizar comparativos entre soluciones de seguridad basándose en resultados relativos, si se integran métricas consistentes se pueden tomar como factores de ROSI.

Existe una relación de factores que afectan al riesgo, entre los cuáles se encuentran: el costo del activo y su valor en el mercado, el número de incidentes ocurridos en el pasado y el costo que estos han representado para la entidad, entre otros.

2.4.3 Riesgos en el manejo de la seguridad de la información

Si bien lo hemos planteado sabemos que en las organizaciones se pueden tener riesgos, los cuáles pueden variar dependiendo de la forma en que se maneja la seguridad de la información. Es posible manejar los riesgos si sabemos hacer una evaluación de ellos, siempre que se trabaje un buen sistema en el manejo de la seguridad de la información se involucrarán tanto las políticas, la estructura de la organización, los procedimientos, los procesos y los activos necesarios.

Pero ¿cómo evaluamos los riesgos? Existen dos maneras para realizarlo; podemos evaluar los riesgos de forma cualitativa o cuantitativa. En la cualitativa no se realizan valores financieros a los activos de la entidad, ni pérdidas previstas, sin embargo se calculan valores relativos. Cuando se utiliza el método cualitativo no se dedica tanto tiempo en intentar calcular cifras financieras para la seguridad de la información y de ésta forma se supera la dificultad de calcular cifras exactas; lo cual es una enorme diferencia con el cuantitativo ya que puede arrojar resultados importantes en poco tiempo aunque su limitación es que la información está sustentada en cifras vagas.

Ventajas e inconvenientes de cada enfoque de administración de riesgos

	Cuantitativo	Cualitativo
Ventajas	– Se asignan prioridades a los riesgos según las repercusiones financieras; se asignan prioridades de los activos según los valores financieros. – Los resultados facilitan la administración del riesgo por el rendimiento de la inversión en seguridad. – Los resultados se pueden expresar en terminología específica de administración (por ejemplo, los valores monetarios y la probabilidad expresada	– Permite la visibilidad y la comprensión de la clasificación de riesgos. – Resulta más fácil lograr el consenso. – No es necesario cuantificar la frecuencia de las amenazas. – No es necesario determinar los valores financieros de

	Cuantitativo como un porcentaje específico). – La precisión tiende a ser mayor con el tiempo a medida que la organización crea un registro de historial de los datos mientras gana experiencia.	Cualitativo los activos. – Resulta más fácil involucrar a personas que no sean expertas en seguridad o en informática.
Inconvenientes	– Los valores de repercusión asignados a los riesgos se basan en las opiniones subjetivas de los participantes. – El proceso para lograr resultados creíbles y el consenso es muy lento. – Los cálculos pueden ser complejos y lentos. – Los resultados sólo se presentan en términos monetarios y pueden ser difíciles de interpretar por parte de personas sin conocimientos técnicos. – El proceso requiere experiencia, por lo que los participantes no pueden recibir cursos fácilmente durante el mismo.	– No hay una distinción suficiente entre los riesgos importantes. – Resulta difícil invertir en la implementación de controles porque no existe una base para un análisis de costo-beneficio. – Los resultados dependen de la calidad del equipo de administración de riesgos que los hayan creado.

2.4.3.1 Cuantificación de la exposición del riesgo

Podemos hablar de un método analítico para calcular la exposición del riesgo el cual toma como factor multiplicativo el costo de un incidente de seguridad (*Single Loss Exposure*), que es estimado anualmente mediante el ARO (*Annual Rate of Occurenc*e). El resultado de este parámetro es la exposición de pérdida anual (*Annual Loss Exposure*). No existe una metodología estándar para estimar el SLE y el ARO, solo existen tablas de actuaría que proporcionan promedios estadísticos basados en daños reales anteriores. Existen algunas tablas que se toman de referencia como son las "*Computer crime and Security Survey*" elaborados por CSI/FBI (*Computer Security Institute / Federal Bureau of Invertigation*).

Exposicion_Riesgo = ALE = SLE * ARO
SLE *Single Loss Exposure*
ARO *Rate of Occurence*

ALE *Annual Loss Exposure*

SLE (expectativa de pérdida simple) es la cantidad total de ingresos que se pierde por una única incidencia del riesgo. Se trata de un importe monetario que se asigna a un único suceso que representa la cantidad de pérdida potencial, en caso de que una amenaza específica aproveche una vulnerabilidad.

ARO (frecuencia anual) es la cantidad razonable de veces que se espera que ocurra el riesgo durante el año.

ALE (expectativa de pérdida anual) es la cantidad total de dinero que la organización perderá en un año si no se toman medidas para mitigar el riesgo. Para calcular este valor se multiplica la expectativa de pérdida simple por la frecuencia anual. La expectativa de pérdida anual es similar al intervalo relativo de un análisis de riesgo cualitativo. Proporciona un valor con el que la organización puede trabajar para presupuestar cuánto costará establecer controles o protecciones para prevenir este tipo de daño y brindar un nivel adecuado de protección. Es importante cuantificar la posibilidad real de un riesgo y el daño, en términos monetarios, que puede causar la amenaza para determinar la cantidad que se puede destinar en la protección contra la posible consecuencia de la amenaza.

2.4.3.2 Expectativa de riesgo

Usar estadísticas externas de (SLE y ARO) pueden carecer muchas veces de valor para la organización ya que no reflejan el comportamiento interno.

Es necesario obtener cálculos reales sobre el costo de un incidente de seguridad (SLE), pues muchas veces las organizaciones ocultan información sobre los incidentes de seguridad que se les presentan. Algunas veces los huecos que se encuentran en las organizaciones sobre seguridad puede que estén presentes pero no son detectados por un tiempo, ya que no tienen impactos en las operaciones diarias de la entidad. Por lo tanto los datos que se encuentran en las tablas pueden ser no tan reales debido a que las organizaciones prefieren ocultar sus problemas para que no sean noticia pública. Es por eso que es recomendable que se desarrollen las propias métricas en el interior de la organización.

2.4.4 Pérdida de la productividad

Una falla de seguridad puede afectar directamente llevándola a una perdida de productividad presentando un impacto serio. Por ejemplo si un sistema se encuentra fuera de línea causa una gran pérdida aunque sean solo unos minutos ya que si multiplicamos el tiempo por todos los empleados que lo utilizan, nos damos cuenta que se perdió mucho tiempo de productividad. Se puede proyectar el número de horas perdidas, en caídas de sistemas anteriores, con el fin de determinar cuál es el costo aproximado para una caída del sistema y de ésta manera podemos tener una base de cálculo para determinar las pérdidas de producción. Una forma de determinarlo es tomar el promedio de las horas trabajadas, más las prestaciones y costos de tiempo extra que afecten al grupo de trabajo y multiplicarlo por el tiempo de caída del sistema. Esta fórmula debe repetirse en todas las áreas de la entidad ya que no todos trabajan igual y varía la perdida de producción.

Con el ejemplo anterior podemos darnos cuenta que si un empleado deja de producir por falta de sistema, la organización esta perdiendo porque aunque la producción esta parada, sigue pagando los salarios de sus empleados sin que ellos estén haciendo algo.

2.4.5 Efectos de la seguridad en la productividad

Esto se puede realizar a través de encuestas. Sin embargo, la encuesta debe estar bien estructurada, para obtener una correlación entre los resultados de la encuesta y la visión financiera. Es decir una buena encuesta nos proporciona respuestas cuantificables. La clave de que una encuesta este bien construida es que al obtener los resultados sean consistentes para poder medir la percepción de los empleados. El crear las preguntas correctamente nos va a arrojar resultados sobresalientes, se tiene que correlacionar los resultados bajo un mismo parámetro.

2.4.6 Cuantificación de la mitigación del riesgo

Determinar la mitigación del riesgo de un dispositivo de seguridad es igual de complicado que medir la exposición del riesgo.

Las soluciones de seguridad son diseñadas para mitigar algunos riesgos, si la solución funciona, la mitigación debe andar cerca del 100% aunque el 85% ya se considera una posición conservadora. Los argumentos anteriores son utilizados para proporcionar un porcentaje fijo a la mitigación del riesgo, aunque tienen algunos problemas estas lógicas ya que los riesgos no son aislados por lo tanto una solución tampoco puede trabajar de forma aislada, porque la existencia y efectividad de otra solución puede tener un mayor impacto, además que las soluciones de seguridad llegan a ser menos efectivas con el tiempo. Aunque un punto es que la implementación de una solución de seguridad en contadas ocasiones no impactará la productividad.

La solución más viable es la de conducir un análisis de seguridad y determinar la valoración de la mitigación que se basa en algoritmos regularmente de redes neuronales que pueden calcular los valores adaptables de la mitigación de riesgos.

2.4.7 Cuantificación del costo de la solución

En este punto debemos suponer que el costo de la solución no solo representa el precio del producto, sino también el costo interno asociado a la implementación de la solución y otros factores que deben ser tomados en cuenta. En este caso una vez más la productividad se encarga de complicar la situación.

La productividad es importante porque la seguridad siempre será considerada dependiendo del costo, dado que algunas soluciones pueden crear barreras que necesitan de otras soluciones para salir adelante.

CAPÍTULO 3

MODELOS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

El éxito que se obtiene en una organización con respecto a la seguridad informática depende de implementar los controles de seguridad adecuados. Para ello es necesario comprender y especificar con precisión los requerimientos de seguridad propios de la organización, siendo éste, uno de los objetivos de los modelos y estándares de seguridad.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde dicha tarea de forma metódica, documentada y basada en objetivos claros de seguridad y, una evaluación de los riesgos a los que está sometida la información de la organización.

3.1 Modelos de seguridad

Los modelos de seguridad son representaciones formales de las políticas de seguridad en las organizaciones, ya que verifican la completitud y su consistencia, así como los mecanismos necesarios para su implementación. Nos ayuda a tener una confianza sobre la validez de un esquema de seguridad; en algunos de los casos a través de una sustentación matemática comprobando de esa manera que los activos son seguros.

Cuando una organización decide tomar un modelo para basarse en él, es importante que tome en cuenta que éste debe ser fácil de comprender, implementar, carente de ambigüedad y capaz de incorporar las políticas de la organización. Siempre que hablamos de la seguridad en la información existen tres propiedades básicas que son tomadas en cuenta, pues nos ayudan a asegurar nuestros activos (Confidencialidad, Integridad y Disponibilidad). Por lo anterior existe una variedad de modelos de seguridad los cuales están divididos dependiendo de lo que se desea proteger pues todas las organizaciones son diferentes y no siempre protegen lo mismo. Por ejemplo, algunas se preocupan más por una posible filtración de información confidencial mientras que otras tratan de proteger la integridad.

Por último cabe mencionar que los modelos no se usan para implementar seguridad si no para evaluar los diseños de seguridad de un sistema, es decir, proporciona una representación semántica que describe las propiedades funcionales y estructurales de la seguridad de nuestro sistema.

3.1.1 Modelos de autenticación

Como lo hemos visto en capítulos anteriores la autentificación es la confirmación de que algo o alguien es quien dice ser, es decir, que un objeto confirme su procedencia o una persona verifique su identidad. Es por eso que los modelos de autenticación están en función de lo que utilizan para la verificación ya sea de los objetos o de las personas.

A continuación se mencionaran algunos modelos dedicados a la autenticación y la forma en que llevan a cabo esa tarea.

3.1.1.1 Modelo de matriz de acceso

El Modelo de la Matriz de Acceso fue propuesto por Lampson como una representación generalizada de mecanismos de protección en sistemas operativos. De este modelo han salido diversas variaciones.

La forma en que trabaja el modelo es con un conjunto de recursos, denominados objetos, cuyo acceso debe ser controlado, y por otro lado se tiene un conjunto de sujetos que acceden a dichos objetos. Se tiene un conjunto de permisos de acceso que especifica los diferentes permisos que los sujetos pueden tener sobre los objetos (normalmente lectura, escritura, etc.)

Se trata de especificar para cada pareja (sujeto, objeto), los permisos de acceso que el sujeto tiene sobre el objeto. Esto se representa mediante una matriz de acceso M que enfrenta todos los sujetos con todos los objetos. En cada celda M[i, j] se indican los permisos de acceso concretos que tiene el sujeto i sobre el objeto j.

Podemos ver a la matriz de accesos como el almacenaje de los estados de protección del sistema; así ciertas operaciones invocadas por los sujetos pueden alterar estos estados.

La figura 3.1 representa una matriz de acceso.

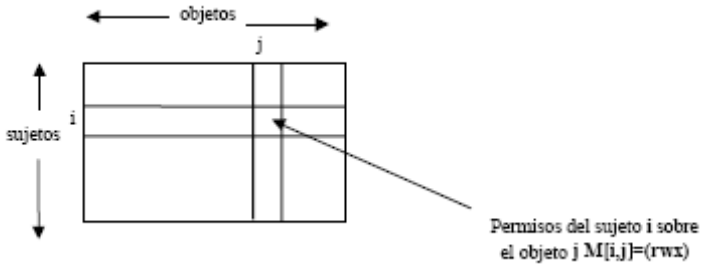


Figura 3.1 Matriz de acceso

3.1.1.2 Modelo HRU

El Modelo HRU fue creado en 1976 por Michael Harrison, Walter Ruzzo y Jeffrey Ullman, basándose en el modelo de matriz de acceso. Su principal objetivo era la protección de los sistemas, verificando quien tiene acceso a que objetos.

HRU es un modelo formal, es decir, cuenta con una demostración para cada una de sus definiciones y teoremas. Está basado en comandos, donde cada comando contiene condiciones y operaciones primitivas.

El modelo nos da diferentes tipos de sistemas de protección para implementar controles de acceso y confidencialidad. Sin embargo solo ve por la protección o confidencialidad de los objetos basándose en la matriz de control de acceso, pero no se preocupa por la integridad y disponibilidad de los datos. Nos permite identificar algunos estados, en los cuales el sistema de seguridad no converge a un estado decisivo, pero permite definir de forma sencilla políticas de seguridad para la organización basándose en la protección de los datos.

3.1.1.3 Modelo Take-Grant

El modelo Take-grant fue desarrollado por A. Jones, R. Lipton y L. Snyder en 1976, éste modelo garantiza que la seguridad de un sistema sea decisivo, sino que lo sea en forma lineal con respecto a la cantidad de objetos y derechos cubiertos por el sistema, es un método que se puede considerar como una variante de la matriz de acceso. Se considera a la matriz como un grafo. Los objetos son nodos y un arco entre nodos indica que el primer objeto puede acceder al segundo. El arco se etiqueta con los permisos de acceso. Se usan dos permisos especiales para modificar el grafo: *take* (tomar) y *grant* (conceder).

El modelo se basa en grafos dirigidos, sus arcos son etiquetados con letras que representan operaciones. A partir de la definición del modelo Take-Grant se han creado diferentes trabajos sobre los cuales se desarrollan algoritmos y casos de estudio sobre posibles situaciones que se puedan presentar dentro de los grafos de protección.

Es importante aclarar que el modelo de seguridad Take-Grant no está orientado hacia algún tipo de sistemas en particular. Es suficientemente abstracto que con algunos ajustes sirve de plataforma a cualquier implementación específica de protección.

El modelo tiene una propiedad importante donde no existe una comunicación y cooperación entre dos sujetos lo que impide conspiraciones. Además de que los objetos así como los sujetos tienen una clasificación asignada, impidiendo de esta manera que la información fluya indebidamente entre niveles.

Las reglas del modelo consisten en que un objeto debe tener asignada la misma clasificación del sujeto de más bajo nivel que puede acceder y el sujeto debe tener al menos el mismo nivel del objeto al que desea acceder.

El modelo Take-Grant tiene algunas limitaciones: no es aceptable bajo ningún concepto la desclasificación o la reclasificación de la información porque de lo contrario la seguridad (y en especial la confidencialidad) resultaría seriamente comprometida.

El modelo de protección Take-Grant para jerarquías no considera que la clasificación de la información pueda ser cambiada, porque de ser así, la seguridad se vería comprometida. Si un usuario tiene acceso a un objeto siempre puede almacenar una copia, y si luego dicho objeto es ascendido, aún el sujeto puede tener acceso a él. Por otro lado, disminuir el nivel de seguridad de un objeto puede comprometer la seguridad dado que un sujeto podría desclasificar información de su nivel para que otro con un nivel inferior pueda accederla.

Jeremy Frank y Matt Bishop modificaron el modelo para identificar los caminos a través de los cuales la información fluye más fácilmente, de esta manera se puede monitorear los nodos, y las conexiones claves para reducir la probabilidad de que ocurran flujos ilícitos de información.

El modelo original no tiene las herramientas suficientes para diferenciar entre dos flujos diferentes, esta deficiencia fue evaluada por Frank y Bishop quienes crearon las reglas de jure y de facto como mecanismos para evaluar cual de los caminos entre dos nodos tienen mayor probabilidad de ser utilizado y establecer controles sobre los sujetos y privilegios.

El modelo no garantiza que la confidencialidad de la información sea una constante. Por tal motivo, para poder garantizar dicho principio de la seguridad, es necesario llevar a cabo modificaciones en las implementaciones y en las derivaciones del modelo formal inicial.

3.1.2 Modelos de confidencialidad

Para algunos modelos su mayor objetivo es proteger la confidencialidad de la organización, como lo explicamos en el capítulo 1, al tener un sistema cumpliendo con el principio de confidencialidad, la información solo puede ser vista por quien tiene derecho y de acuerdo al nivel de acceso permitido. Los siguientes modelos están basados en el esquema militar. Este esquema garantiza la confidencialidad, debido al nivel de sensibilidad de la información que es manejada por ellos, solo algunas personas que tienen un nivel de clasificación que por lo menos es superior o igual a la información presentada tendrán acceso a esta. Esto lo veremos claramente en el modelo Bell LaPadula (BLP), el cual se explicará posteriormente.

Otro modelo de confidencialidad es el modelo Harrison-Ruzzo-Ullman el cual es una modificación del modelo BPL.

3.1.2.1 Modelo Bell-LaPadula

El modelo Bell LaPadula (BLP) fue desarrollado en 1976 por David Bell y Len LaPadula de la organización Mitre fundada por el Departamento de Policía de los E.E.U.U tomando en cuenta los diferentes niveles de seguridad con los que contaba la defensa. Es uno de los primeros modelos formales de seguridad multinivel.

Este modelo clasifica por niveles de seguridad a los objetos y los usuarios:

- Secreto superior
- Secreto
- Confidencial
- Sin clasificar

Busca proteger la confidencialidad de la información y no toma en cuenta la integridad y disponibilidad.

Los componentes definidos por el modelo son:

- ✓ Sujetos: las entidades del sistema, incluidos usuarios y procesos
- ✓ Objetos: las estructuras de información, que almacenan la información del sistema
- ✓ Modos de acceso: como un sujeto interactúa con un objeto
- ✓ Niveles de seguridad: cada objeto tiene una clasificación y cada sujeto un nivel

El modelo Bell LaPadula tiene tres propiedades principales:

1. Propiedad básica: Un sujeto sólo puede leer los objetos que se encuentre por abajo o igual al nivel de seguridad que tiene el sujeto. La lectura hacia arriba está prohibida. (Fig. 3.2)

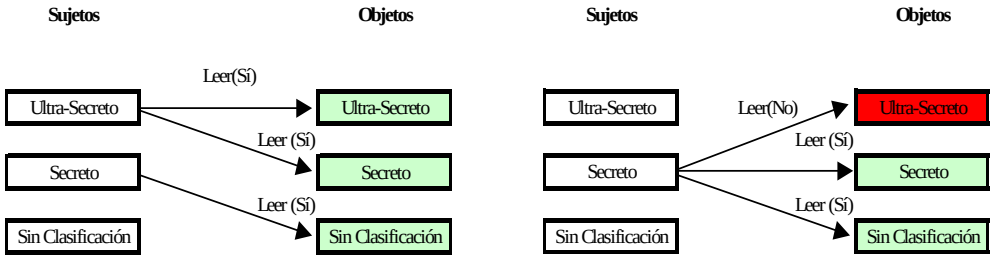


Figura 3.2 Propiedad Básica

2. Propiedad de estrella: Existe la escritura cuando el nivel de seguridad del sujeto es menor o igual que el nivel de seguridad del objeto. Es decir, la escritura hacia abajo está prohibida.(Fig. 3.3)

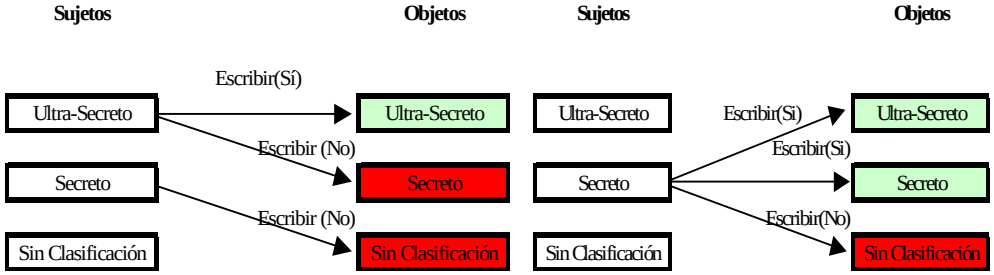


Figura 3.3 Propiedad Estrella

3. Propiedad de acceso discrecional: basada en la matriz de acceso en el cual se establecen los permisos que un sujeto tiene sobre un objeto. (Fig. 3.4)

		Objetos	
		Archivo X	Archivo Y
Sujetos	Juan	Leer	Leer/Escribir
	Pedro	-	Ejecutar

Figura 3.4 Propiedad matriz

Este es un modelo forma algebraico que parte de una hipótesis de un estado seguro, definiendo reglas que generan estados seguros. Está basado en máquinas de estados finitos, consiste en la definición de un conjunto de variables de estado, funciones de transición y un estado inicial considerado seguro, de esta manera podemos probar que todas las transiciones son seguras y que nos llevan a estados seguros.

3.1.3 Modelos de integridad

Históricamente hablando sobre la seguridad informática, hubo mayor atención a la confidencialidad, pero con el transcurso de los años, el NIST (Nacional Institute of Science and Technology) se enfoca en la integridad creando modelos que toman importancia sobre todo en el sector comercial. Si hablamos de seguridad en las organizaciones no tiene el mismo significado, los modelos buscan resolver aspectos diferentes de la seguridad, es por eso que la comparación entre modelos no es siempre directa ni evidente.

Los modelos que se mencionan a continuación sostienen que la integridad es más importante que la confidencialidad basándose en sistemas comerciales.

Cuando hablamos de integridad nos referimos a la forma de proteger la información de posibles cambios intencionales o accidentales no autorizados durante el flujo de la información o cuando se encuentre almacenada, los modelos de integridad, brindan mecanismos de protección para prevenir las modificaciones no autorizadas de tal manera que la información se encuentre integra cuando la requieran.

Para alcanzar los objetivos de la integridad, es necesario que un conjunto de servicios de seguridad incorporen las propiedades necesarias al igual que un marco de trabajo que permita incluir dichas propiedades. Las propiedades de seguridad requeridas para la integridad son: el control de acceso, las auditorias y la responsabilidad.

3.1.3.1 Modelo de integridad Biba

El modelo Biba fue creado en 1977 por K. J. Biba. Está orientado a la seguridad de la integridad de los datos, centrándose en la protección contra usuarios de un nivel inferior que desean escribir en cualquiera de los niveles superiores, con este modelo un usuario de bajo nivel de seguridad no podrá sobrescribir documentos altamente secretos, es por eso que se adopta un conjunto de políticas de integridad.

Biba se basa en modelos de máquinas de estados que buscan representar formalmente los estados de un sistema. Su uso hace referencia a los siguientes puntos:

- Definir el conjunto de estados que están involucrados en el proceso de seguridad.
- Verifica todos los estados de transición que llevan de un estado seguro, a uno igualmente seguro.
- Verifica el estado inicial de sistema “seguro”.

La clasificación de los objetos y usuarios es por niveles de seguridad igual que el Bell-Lapadula pero una diferencia entre ellos, es que el usuario puede escribir en su mismo nivel o por debajo de su nivel, además de leer un objeto de su nivel o de nivel superior.

Cuando se utiliza el modelo Bell-Lapadula con éste se garantiza una confidencialidad e integridad, pero se limita la facilidad de compartir recursos.

Biba es un modelo multinivel, donde a los usuarios y objetos se les asigna un nivel de seguridad escogido de un conjunto común de niveles. Se establece un conjunto de reglas para verificar si una transición producirá o no un estado seguro. Los objetos son asignados a clases de integridad dependiendo del daño que sufrirían si fueran modificados incorrectamente, mientras los usuarios son asignados a clases de integridad dependiendo de su veracidad.

Biba esta determinado por tres reglas que tienen por objeto evitar las lecturas abajo y las escrituras arriba de un nivel de seguridad dado a un sujeto.

La política de integridad estricta se caracteriza por tres propiedades:

1. La primera propiedad nos dice que un sujeto puede observar a un objeto, si el sujeto tiene un nivel de integridad menor o igual que el nivel de integridad del objeto (Fig. 3.5).

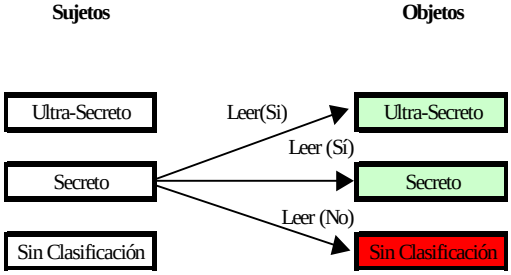


Figura 3.5 Propiedad de lectura hacia arriba

2. La segunda propiedad nos dice que un sujeto puede modificar un objeto, si el objeto tiene un nivel de integridad menor o igual que el nivel de integridad del sujeto (Fig. 3.6).

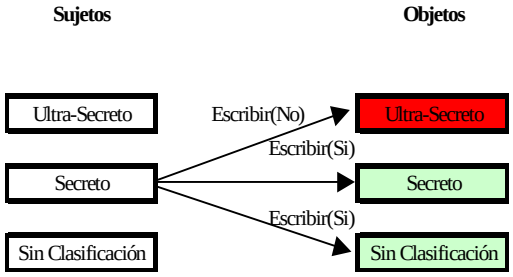


Figura 3.6 Propiedad de escritura hacia abajo

3. Por ultimo para que un sujeto 1 invoque a un sujeto 2, el sujeto 2 debe tener un nivel de integridad menor o igual que el nivel de integridad del sujeto 1.

Con estas propiedades podemos observar que un sujeto no puede observar a un objeto de menor integridad y no puede modificar a un objeto de más alta integridad, así como un sujeto no puede

invocar a otro sujeto de más alta integridad, tratando de prevenir que el sujeto invoque cualquier modificación indirecta de objetos de más alta integridad.

3.1.3.2 Modelo de integridad de Clark-Wilson

Entre los años 1987 y 1989 se creó el modelo Clark-Wilson por David D. Clark y David R. Wilson, su objetivo era demostrar que en los sistemas comerciales era más importante la integridad que la confidencialidad.

Se enfoca en dos controles importantes en el sector comercial.

a) Transacciones correctas: Garantiza que un usuario no puede modificar información arbitrariamente, sólo permite modificación en situaciones específicas y en una forma determinada.
b) De separación de obligaciones: Trata de mantener estable la información al separar todas las operaciones o acciones en diferentes partes que son realizadas por diferentes usuarios.

Aunque no se considera un modelo altamente formal ayuda a establecer los requerimientos de la integridad.

Está orientado a sujetos, objetos y un nuevo elemento llamado "programas", a estos tres se les conoce como el Acceso Triple el cual impide que usuarios autorizados modifiquen datos o programas.

Los datos que se manejan se dividen en dos grupos:

- Elementos de Datos Restringidos (CDIs): elementos que deben mantenerse íntegros.
- Elementos de Datos No Restringidos (UDIs): Elementos u objetos no protegidos por políticas de integridad pero que pueden llegar a ser CDIs.

Al ser divididos los datos se tienen dos diferentes procedimientos para protegerlos:

- Procedimiento de Verificación de Integridad (IVP), durante el proceso de los datos CDIs se confirma que se encuentran en un estado seguro.
- Procedimiento de Transformación (TP), Mantiene la consistencia interna y externa de la información, se encarga de que el sistema pase de un estado válido a otro. El sistema debe asegurar que solo los TPs pueden manipular a los CDIs.

Si comparamos el modelo con otros podemos darnos cuenta que no se definen niveles de seguridad para la información sino que toma en cuenta los programas que un usuario puede ejecutar, los cuales manejan la información.

Comparando el modelo Clark-Wilson con el Orange Book (libro naranja), podemos ver que da permisos de ejecución a ciertos programas. La diferencia entre estos mecanismos es muy clara ya que con los controles planteados por el Orange Book, los usuarios que tienen determinados permisos sobre un objeto pueden utilizarlos de cualquier forma, mientras que en Clark-Wilson los usuarios se someten a lo que los programas ejecuten, esto se refleja en la separación de obligaciones, donde un usuario modifica un objeto solo a través de un conjunto de transacciones definidas para ese usuario

(programas), y otros usuarios con otras obligaciones tendrán acceso a un conjunto diferente de transacciones. Sin embargo el modelo Clark-Wilson tiene algunas desventajas ya que al tener un conjunto de programas los cuáles modifican los objetos, permite que los datos se encuentren más accesibles.

3.1.4 Modelos híbridos

Los Modelos Híbridos es la combinación de las propiedades de seguridad integridad, confidencialidad y disponibilidad. Se puede decir que son modelos más robustos y seguros ya que no solo protegen algo en específico sino que se convierte en una seguridad global.

3.1.4.1 Modelo Chinese Wall

Brewer y Nash desarrollaron en 1989 el modelo Chinese Wall (Muralla China) el cuál se puede analizar como un código de prácticas que deben ser seguidas por analistas del sector comercial. Existen políticas de seguridad dentro de este modelo que nos ayudan a garantizar grados de confidencialidad para prevenir el flujo de datos confidenciales.

Una característica de este modelo a diferencia de otros es que no tiene políticas independientes entre usuarios y objetos, ya que los dos tienen las mismas características y son tratados igual. Además las reglas aplicadas en este modelo son una alternativa para garantizar grados de confidencialidad.

Si comparamos los modelos anteriores con el modelo Chinese Wall, nos damos cuenta que este provee una mayor seguridad en la confidencialidad de la información, ya que los datos que se manejan no pueden ser leídos por personas no autorizadas, sin embargo, si llegasen a obtener la información el modelo garantiza que no podrá conocer su contenido.

La política de Chinese Wall permite el acceso a la información a aquellos que no representen competencia, es decir, pueden compartir información siempre y cuando no generen un conflicto de interés para la organización.

En el siguiente cuadro se hace una comparación exhaustiva entre los modelos Chinese Wall y Clark-Wilson.

3.2 Normatividad y regulaciones

Hoy en día, las organizaciones necesitan identificarse con las tecnologías de seguridad para lograr y mantener el cumplimiento de las regulaciones actuales como la Ley de Portabilidad y Contabilidad de los Seguros de Salud (HIPAA), la ley Sarbanes-Oxley y la ley Gramm-Leach-Bliley (GLBA), las cuáles se mencionarán posteriormente.

El tener que regirse por normas y regulaciones ha llevado a las instituciones a preocuparse por el cumplimiento de éstas, permitiéndoles tener una ventaja competitiva ya que aumenta la confianza de los clientes.

La normatividad son reglas, las entidades deben de ajustarse a estas para obtener seguridad en las TI, llevando a cabo procedimientos que afectan amplias áreas de la privacidad de datos, seguridad, retención, protección y responsabilidad.

Las regulaciones abordan un asunto diferente y tienen sus propios requisitos básicos para el cumplimiento.

3.2.1 Internacionales

Para que las organizaciones tengan un crecimiento y liderazgo internacional es necesario regirse de las normas internacionales. Estas surgieron al evaluar los riesgos y buscaron la manera de mitigarlos desarrollando directivas y sistemas para su cumplimiento.

Cualquier organización puede sufrir ataques, afectando no solo a la organización sino a terceras personas, por esa razón existen diferentes leyes las cuáles les exigen proteger la información identificable de índole personal.

Las leyes internacionales obligaron a las empresas a ejecutar un enfoque mucho más riguroso con respecto a sus controles internos en el proceso de auditoría y generación de informes.

Las organizaciones que desean cumplir las regulaciones necesitan contar con sistemas seguros.

Sin embargo algunas leyes son imprecisas en términos de qué tienen que hacer las entidades para alcanzar verdaderamente el cumplimiento. La razón por la que algunas regulaciones son imprecisas es porque tienen que aplicarse distintos tipos de organizaciones.

Sin importar lo que la entidad decida hacer para alcanzar y mantener el cumplimiento, es necesario que pueda justificar sus esfuerzos a través de documentación, informes confiables y una buena auditoría de contenido, es decir todo gira en torno a la documentación.

3.2.1.1 Sarbanes Oxley

En Estados Unidos hubo grandes escándalos financieros; donde las empresas falseaban la información para poder publicar resultados positivos aunque la verdad de la corporación fuera totalmente distinta y estuviera perdiendo dinero.

Se ha hecho creer en algunas ocasiones que las acciones tienen un valor mayor al que en verdad tienen y cuando esto se descubre el precio de las acciones, baja de manera estrepitosa hasta llegar hacer quebrar a una empresa. Es por eso que preocupados por este fenómeno, se propuso al congreso de los Estados Unidos establecer ciertas normas o reglas impidiendo que la información financiera de las organizaciones fuera alterada de manera dolosa por los CFO o CEO o bien los accionistas estuvieran enterados de manera fehaciente del comportamiento del valor de sus acciones. Así fue como se creó la Ley de Sarbanes-Oxley (SORBOX o SOx) promulgada el 30 de julio de 2002. Su ámbito de aplicación es para todas aquellas empresas cuyos valores, acciones y obligaciones, coticen en Wall Street.

Ésta ley está compuesta por 11 títulos, definiendo las responsabilidades de administración en los reportes anuales y semestrales, el ambiente del control, gestión de riesgo, el monitoreo y la medición de las actividades de control. Le exige a las organizaciones que cotizan en el mercado de acciones estadounidense, certifiquen sus controles internos y la precisión de sus informes financieros. Surgiendo de esta manera la seguridad de la información como una base fundamental para la conformidad. Sin las medidas de seguridad apropiadas, las corporaciones no podrán cerrar sus libros y controles internos con confianza.

Podemos decir que el área de las TI es el corazón de cualquier organización por lo que el CIO es el responsable de ofrecer las diferentes herramientas y estrategias para poder hacer cumplir la ley. Es por eso que existe una gran relación entre la ley de Sarbanes-Oxley y las TI porque toda la información de la organización está almacenada y operada por ésta.

Esta Ley no solo afecta a Estados Unidos si no que ya está dentro de las organizaciones que cotizan en las Bolsas de Valores de los Estados Unidos. Por lo que las organizaciones mexicanas no están exentas y deben de asegurar sus procesos y certificarse en diferentes normas internacionales.

3.2.1.2 Gramm Leach Bliley

La sociedad impone leyes sobre la seguridad de la información de las organizaciones, como sucedió con la ley Gramm-Leach-Bliley (Ley federal sobre la privacidad), aprobada en 1999, la cual regula lo que las empresas de servicios financieros pueden hacer con la información personal y confidencial que recopilan como parte de sus actividades de asesoría de inversiones. Exigiendo la privacidad y protección de los registros de los clientes que se encuentran almacenados en instituciones financieras.

Además que esta ley moderniza el panorama financiero estadounidense, contiene elementos de privacidad y seguridad significativos para los individuos.

En cuestión de la gestión de seguridad de TI

- Proporciona un aviso de privacidad a todos los puntos de aplicación en línea
- Adopta en la organización políticas y procedimientos adecuados para proteger los datos del cliente según lo especificado en la ley GLBA (Ley de Gramm-leach-Bliley)
- Se ocupa de evaluaciones de riesgo regulares de terceras partes para la ingeniería social, los sistemas y las garantías lógicas en la organización
- Asegura que todos los socios y otras terceras partes estén adecuadamente seguros y adhieran a los estándares de seguridad validados.
- Protege contra cualquier amenaza o peligro anticipado que afecte a la seguridad o integridad de los expedientes del cliente.
- Protege contra el acceso no autorizado o el uso de estos expedientes o la información que pudiere ocasionar un daño o inconveniente substancial a un cliente.

3.2.1.3 California Senate Hill (SB 1386)

El primero de julio del 2003 se aprobó en California la ley de California Senate Hill (SB 1386) sobre notificación en la vulneración de las medidas de seguridad. Esto debido a que un año antes se suscitó un incidente dentro de sistema del gobierno estatal de California, en el cual ingresaron hackers a la información personal de la nómina de más de 200,000 empleados estatales exponiéndolos al fraude y al robo de identidad sin embargo el gobierno avisó a los afectados semanas después de lo ocurrido.

Debido a la importancia que ha cobrado identificar la vulneración de los datos personales y en respuesta a la creciente preocupación relativa a la comunicación de dichas vulnerabilidades a los afectados, esta ley obliga a cualquier entidad o persona que almacena o transmite datos personales de residentes del estado de California a notificar a los residentes del Estado cuyos datos personales puedan haber sido comprometidos por un problema de seguridad. Con esta ley se impulsa a las organizaciones

a adoptar tecnologías de cifrado y mecanismos de respuesta a incidentes de seguridad para así evitar la carga asociada con una notificación deficiente en caso de tales abusos.
Con ésta ley toda empresa que de a conocer de forma accidental u de otra forma, información personal de cualquier residente de California, debe revelar este hecho a la persona afectada dentro de un período razonable.

3.2.1.4 Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA)

El "Health Insurance Portability and Accountability Act" (HIPAA) conocida como la Ley de Portabilidad y Responsabilidad del Seguro Médico, es una Ley Federal que fue aprobada el 16 de agosto de 1996 por el Congreso de Estados Unidos. Se concentra en la protección de los datos del paciente y abarca los tres puntos del triángulo CID (Confidencialidad, Disponibilidad e Integridad)

La meta fundamental de la ley es facilitar a las personas que mantengan un seguro médico, proteger la confidencialidad y la seguridad de la información del cuidado médico y ayudar a la industria del cuidado de la salud a controlar los costos administrativos.

HIPAA se divide en cinco títulos o secciones, cada título trata un aspecto único de la reforma del seguro de salud.

El Título I es la movilidad ("portabilidad"), el cual permite a las personas llevar su seguro médico de un trabajo a otro para que no tengan un lapso en la cobertura. También restringe a los planes médicos de requerir condiciones preexistentes a personas que cambian un plan médico a otro.

El Titulo II se conoce como la Simplificación Administrativa y tendrá un impacto mayor para los proveedores. Se diseñó para:

- Combatir el fraude y abuso en el cuidado de la salud.
- Garantizar la seguridad y la privacidad de la información médica.
- Establecer estándares para la información y transacciones médicas.
- Reducir el costo del cuidado médico mediante la estandardización de la manera en que la industria comunica la información.

Título III – Disposiciones de Salud Relacionadas a Impuestos

Título IV – Aplicación y Cumplimiento de los Requisitos de Planes Grupales de Salud

Título V – Retenciones de Ingresos

No sólo los proveedores de salud y las empresas de seguros se ven afectadas por la HIPAA. De hecho, la legislación exige que cualquier entidad que maneje información sobre pacientes cumpla con la regla de privacidad de la HIPAA. Esto incluye a los empleadores que ofrecen beneficios de atención de salud a sus empleados, al igual que las instituciones financieras que pueden actuar como cámaras de compensación para las transacciones, convirtiendo las transacciones no tradicionales en transacciones estándar y viceversa.

3.2.1.5 Derechos de propiedad intelectual y patente

El término derechos de propiedad intelectual son un conjunto de normas legales utilizadas para regular el uso del "trabajo creativo", para que los inventores o artistas protejan sus obras y no pierdan el control sobre sus creaciones o ideas de su intelecto. Muchos lo llaman como un contrato social entre el autor y el público o entre el inventor y la sociedad.

La propiedad intelectual se divide en dos categorías: la propiedad industrial, que incluye las invenciones (protegidas por patentes) y el Copyright o derecho de autor, que en términos generales cubre las obras de la inteligencia en el ámbito literario, artístico o científico.

Las leyes de propiedad intelectual protegen las obras literarias, artísticas y científicas que cumplen los requisitos de originalidad y creatividad, no siendo objeto de protección las ideas, fórmulas matemáticas, obras no originales y en general todo aquello que no cumpla con los requisitos establecidos en la Ley.

Una patente es un derecho exclusivo concedido a una invención, esto quiere decir que si un producto o procedimiento aporta, una nueva manera de hacer algo o una nueva solución técnica a un problema, y es susceptible de ser explotado industrialmente, puede ser patentado siempre y cuando satisfaga determinados requisitos. Una de las finalidades de la legislación sobre las patentes es inducir al inventor a revelar sus conocimientos para el avance de la sociedad a cambio de la exclusividad durante un periodo limitado de tiempo.

Mientras que los derechos de autor o copyright fueron diseñados para proteger las expresiones de contenido, las patentes protegen el contenido en sí mismo y otorgan monopolio sobre su uso.

Los derechos de propiedad tienen un tiempo de vida el cuál dependerá del tipo de derecho (moral o patrimonial, de autor o conexo), que por regla general los derechos morales son perpetuos y los patrimoniales expiran según el Convenio de Berna después de 50 años tras la muerte del autor sin embargo algunos países de la unión Europea establecen un plazo de 70 años *post mortem auctoris*. Una vez terminado ese plazo la obra se considera de dominio público, siendo posible la libre utilización de la misma, pero respetando los derechos morales del autor, en particular el de reconocimiento de la autoría.

Durante el siglo XX tras la convención de Berna se funda el BIRPI (*Bureaux internationaux réunis pour la protection de la propriété intellectuelle*), actualmente llamado OMPI (Organización Mundial de la Propiedad Intelectual). La cual fue creada para velar por la protección de los derechos de los creadores y los titulares de propiedad intelectual a nivel mundial y contribuir a que se reconozca y se recompense el ingenio de los inventores, autores y artistas.

La Organización Mundial de la Propiedad Intelectual (OMPI), define que la propiedad intelectual le permite a su propietario o titular disponer de su creación como le plazca y ninguna otra persona física o jurídica podrá disponer legalmente de su propiedad sin su consentimiento, sin embargo el ejercicio de este derecho está sujeto a limitaciones.

3.2.2 Nacionales

El delito informático implica actividades criminales, los cuales se han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho, tal como se comentó en el apartado 1.5. Sin embargo es necesario profundizar más al respecto en el ámbito nacional.

En México no existe normatividad o legislación alguna que hable de manera clara y sin lugar a controversias sobre el delito informático.

El mismo concepto de delito informático no está tipificado en la legislación mexicana, sin embargo la Organización para la Cooperación y el Desarrollo Económico definió en 1993 al delito informático como: "Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

La concepción de la definición no es muy clara por lo que los expertos han enriquecido está definiendo al delito informático como: "Delito o crimen informático es toda interrupción, uso indebido, modificación, o fabricación de datos ajenos que se encuentren en sistemas de computación, sin autorización expresa o implícita de su dueño y/o de quien ostente la propiedad intelectual, con el objeto de obtener un provecho económico o no".

Diversos temas de la seguridad se tocan en la legislación mexicana, de manera vaga y poco clara, lo que representa un inconveniente grave al no contar con una figura bien definida sobre el delito informático. Esto permite dar diferentes interpretaciones a la ley y lo peor no tener de manera sólida un respaldo jurídico ante eventualidades.

De manera conceptual es posible clasificar por el tema de seguridad informático tratado, en las diferentes legislaciones de la Federación Mexicana, haciendo nuevamente hincapié, que son dispersas, no son claras y que están lejos de cubrir las necesidades actuales en referencia al uso adecuado de las Tecnologías de la Información y el delito relacionado a ellos. Esta clasificación la podemos ver en la figura 3.7.

A continuación se presentan un compendio de los artículos referentes a la seguridad informática de diversos códigos y leyes federales y estatales vigentes en México.

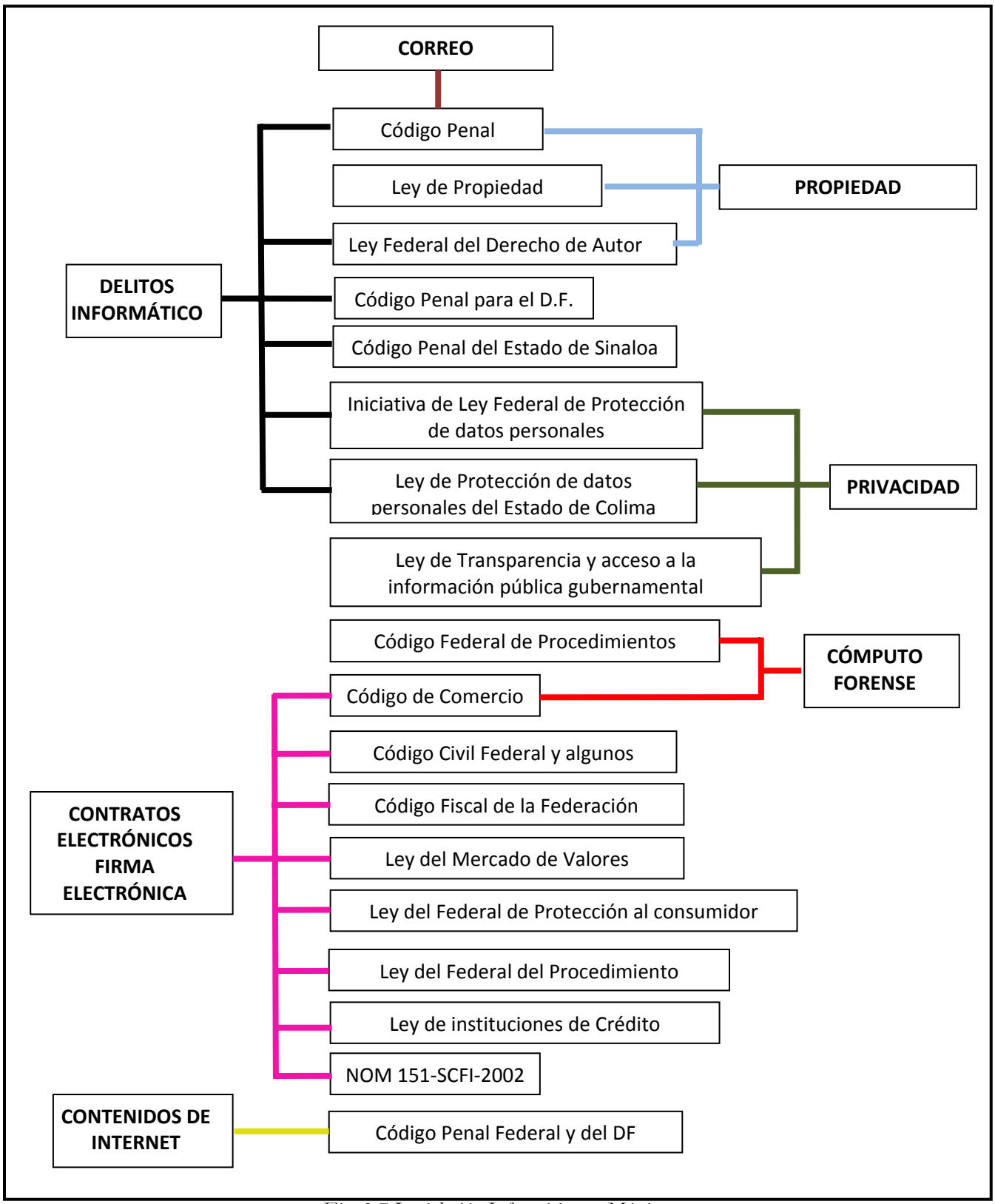


Fig. 3.7 Legislación Informática en México

3.2.2.1 Sobre delitos informáticos

- Acceso no autorizado a sistemas o servicios y destrucción de programas o datos.

Código Penal Federal, artículos 211 bis 1 a 211 bis 7.

Conducta	Pena
Destruir información sin autorización -Si se trata de sistemas o equipos del Estado -Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	-6 meses a 2 años de prisión, 100 a 300 días multa -1 a 4 años y 200 a 600 días multa -6 meses a 4 años de prisión, 100 a 600 días multa
Conocer o copiar información sin autorización -Si se trata de sistemas o equipos del Estado - Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	-3 meses a 1 año de prisión, 50 a 150 días multa -6 meses a 2 años de prisión, 100 a 300 días multa -3 meses a 2 años de prisión, 50 a 300 días multa
Destruir información cuando se tenga autorización para el acceso -Si se trata de sistemas o equipos del Estado -Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	 -2 a 8 años prisión y a 300 a 900 días multa -6 meses a 4 años de prisión y 100 a 600 días multa
Conocer o copiar información cuando se tenga autorización para el acceso -Si se trata de sistemas o equipos del Estado -Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero	 -1 a 4 años de prisión y 150 a 450 días multa -3 meses a 2 años de prisión y 50 a 300 días multa

- Fraude mediante el uso de la computadora y la manipulación de la información que éstas contienen.

Código Penal del Estado de Sinaloa, artículo 217 fracción I.

Comete delito informático, la persona que dolosamente y sin derecho: Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información.

Código Penal para el Distrito Federal, artículo 231.

"Se impondrán las penas previstas en el artículo anterior, a quien: ….XIV para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución"

- Reproducción no autorizada de programas informáticos.

Ley Federal del Derecho de Autor, artículo 11.

Establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que están los programas de cómputo. La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas.

- Uso no autorizado de programas y datos.

Ley Federal del Derecho de Autor, artículos 107 al 110.

Esta Ley protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades, la información privada de las personas contenida en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo consentimiento de la persona de que se trate.

Ley de Protección de Datos Personales del Estado de Colima.

Los principios bajos los cuales deberán manejarse los datos personales, se destaca:
Sólo podrán obtenerse y ser sujetos de tratamiento cuando se han adecuado, pertinentes y no excesivos. Deben ser correctos y actualizados. Deberán obtenerse por medios lícitos será necesario el consentimiento del interesado.

- Intervención de correo electrónico y obtención de información que pasa por el medio.

Código Penal del Estado de Sinaloa, artículo 217 fracción II.

Comete delito informático, la persona que dolosamente y sin derecho: Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Código Penal Federal, artículo 167 fracción VI.

Sanciona con 1 a 5 años de prisión y 100 a 10000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alambradas, inalámbricas o de fibra óptica, sean telegráficas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. Aquí tipificaría el interceptar un correo antes de que llegue a su destinatario, pero no el abrir el buzón o los correos una vez recibidos.

3.2.2.2 Sobre contratos electrónicos

La Ley de Instituciones de crédito y la Ley del Mercado de Valores, regulan el uso de medios electrónicos para la realización de sus operaciones.

El Código de Comercio, a partir del 2003, reconoce expresamente la contratación electrónica, regulando la creación de entidades certificadoras para asegurar la autenticidad de mensajes de datos y firma electrónica.

La Ley Federal de Protección al Consumidor protege como confidencial la información que se proporciona al proveedor y obliga a éste a dar teléfono y domicilio físico.

El Código Civil Federal y algunos Estatales, regulan como consentimiento expreso el manifestado por medios electrónicos y equiparan la oferta hecha entre presentes a la realizada por estos medios.

3.2.2.3 Otras normatividades

Para la protección de la privacidad y de la información en México se tienen esfuerzos importantes como son:

- Ley Federal de Protección al Consumidor.
- Ley Federal del Derecho de Autor.
- Ley de Instituciones de Crédito.
- Iniciativa de Ley Federal de Protección de Datos Personales.
- Ley de Protección de Datos Personales del Estado de Colima.

Con respecto al Cómputo Forense, tanto el Código de Comercio, como la Ley de Instituciones de Crédito, la Ley del Mercado de Valores y el Código Federal de Procedimientos Civiles, le otorgan valor probatorio a los documentos o instrumentos que se obtengan por medios electrónicos.

Finalmente en los Contenidos de Internet, prácticamente no se tiene regulación, con la excepción de la pornografía infantil.

3.2.2.4 Normas internas de la organización

En la actualidad existen organizaciones que no están certificadas con algún estándar, sin embargo llevan a cabo normas de manera voluntaria u obligatoria para poder prevenir, proteger y manejar los riesgos de diferentes daños.

Con las normas internas de la organización pueden informar al mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

Sin embargo las normas internas llegan a ser insuficientes cuando se quiere diferenciar sus productos, procesos o servicios en el mercado nacional e internacional, con el objetivo de alcanzar mayor competitividad.

3.3 Estándares actuales de seguridad informática

Cuando una organización desea desarrollar una política o norma para estandarizar sus procesos y controles es importante hacer un análisis de los diferentes estándares para que se escoja el que mejor se acople a las necesidades de la empresa. Para realizar éste análisis es necesario evaluar la organización en cuanto a su trayectoria, reconocimiento en el dictado de estándares, investigar sobre las implementaciones efectuadas del estándar y sus resultados, analizar el contenido de los estándares con una visión técnica, determinar la aplicabilidad de los estándares al modelo de realidad propia, seleccionar el estándar que mejor cumpla con las expectativas y por último alinearse al estándar seleccionado.

El término estándar es un conjunto de instrucciones y requisitos. Los estándares podemos dividirlos en aquellos que son una especificación formal desarrollada es decir aprobada por un organismo de normalización (ejemplo ISO, Organización Internacional de Normalización) o bien un estándar de facto o "de propiedad" el cuál es adoptado en el mercado sin ninguna normalización formal. Cualquiera tipo de estándar puede requerir la adquisición de una licencia para el uso de los derechos de la propiedad intelectual.

Los estándares abiertos son conjuntos de instrucciones y requerimientos técnicos disponibles al público, desarrollados o aprobados mediante un proceso de consenso, que ha sido ampliamente examinado y acordado por una organización voluntaria de fijación de estándares regidos por el mercado. Ésta se publica con el detalle suficiente para permitir diversas implementaciones y aquéllos que la desarrollan otorgan todos los derechos de patente necesarios para implementarla a todos los que lo hagan de manera razonable y no discriminatoria.

3.3.1 Orientados al análisis de riesgos

La sistematización y la automatización de procesos en las organizaciones no solo han involucrado las áreas operativas, sino que también comprende a los departamentos administrativos y organizativos, creando la aparición de nuevos riesgos asociados. Por todo esto se han creado métodos, herramientas y técnicas que permiten evaluar y medir los riesgos de la sistematización; dichos estándares son reajustados continuamente para la protección y resguardo de procesos, los cuáles se van adaptando conforme pasa el tiempo.

La orientación al riesgo es la más satisfactoria desde el punto de vista teórico, pero puede ser cara y no resulta fácil de manejar a nivel técnico.

3.3.1.1 OCTAVE

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) es un estándar que nos ayuda a evaluar las vulnerabilidades y amenazas existentes; en los activos y las operaciones críticas dentro de las organizaciones.

En la siguiente figura podemos observar las fases que deben desarrollarse para cumplir con ésta metodología:

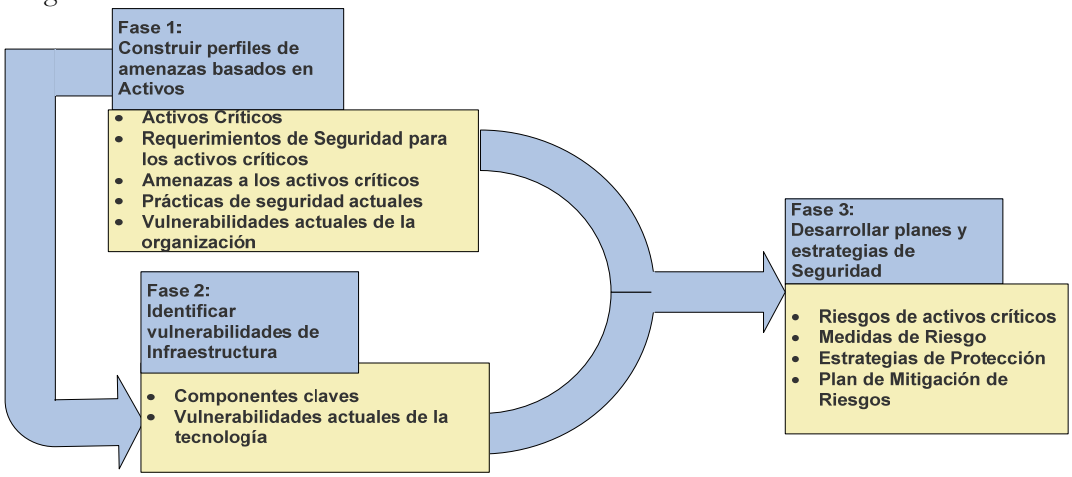


Figura 3.8 Fases de OCTAVE

Se basa en la planificación estratégica y la evaluación técnica de la seguridad, es decir, trabajan en conjunto el departamento de TI con los operativos para localizar las necesidades de seguridad de la organización. Este equipo se basa en los conocimientos del personal para definir cuál es el estado actual de la seguridad, identificar los riesgos para los activos críticos, y establecer una estrategia de seguridad.

3.3.1.2 MAGERIT

En 1997 se publicó la primera versión de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) la cuál es una herramienta metodológica, promoviendo su utilización como respuesta a la percepción de que la Administración depende de forma creciente de las TI para el cumplimiento de su misión.

La razón por la que aparece MAGERIT surge de la necesidad de minimizar ciertos riesgos que se generan al usar los medios electrónicos, informáticos y telemáticos, que son un beneficio para las organizaciones pero que requieren de medidas de seguridad para que no se vuelvan un problema.

Los objetivos que tiene ésta herramienta es concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de controlarlos, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas para mantener los riesgos bajo control y por último apoyar la preparación de la organización para procesos de evaluación, auditoría, certificación y acreditación.

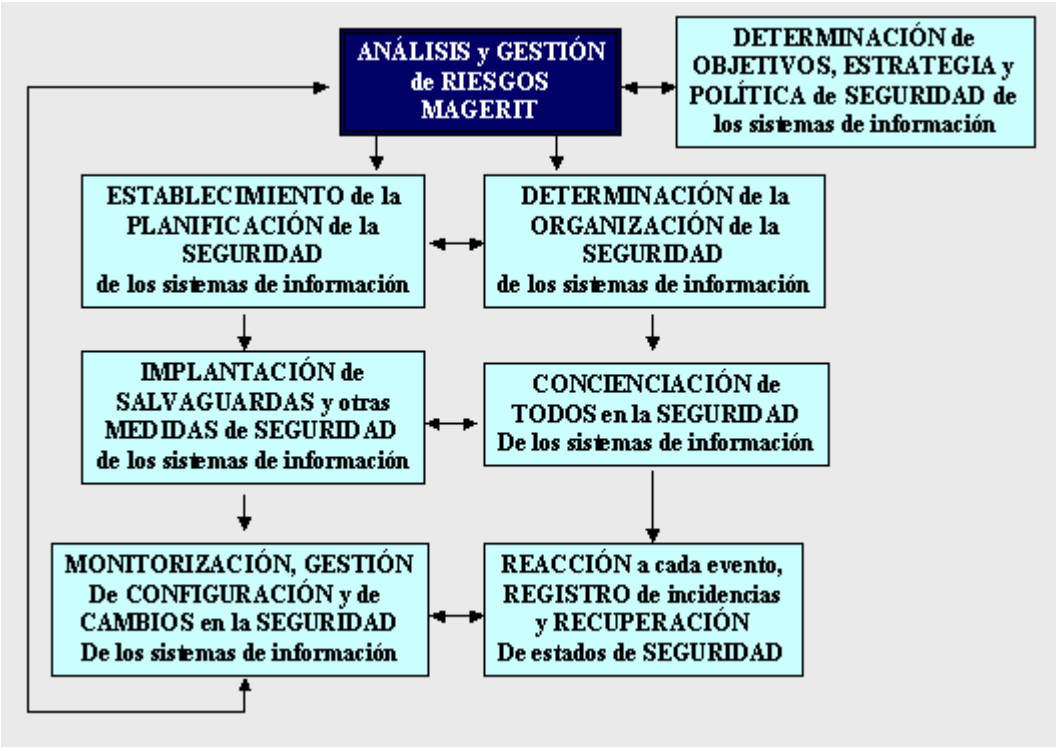


Figura 3.9 Proceso de Magerit

En la figura No. 3.9 se muestra todo el proceso que se lleva a cabo cuando se implementa MAGERIT dentro de la organización.

El uso de las TI son oportunidades para las empresas pero también implican ciertos riesgos que deben minimizarse con medidas de seguridad, para ello se requiere de un análisis de riesgos para identificarlos como lo hemos explicado anteriormente. MAGERIT es un método formal para obtener un mapa de todos los riesgos que se desean controlar y representar, lo que ayuda a tomar las medidas apropiadas que deben adoptarse para controlar estos riesgos.

3.3.1.3 BS 7799-3

En el año 2006 BSI (*British Standards Institution*) publicó la tercera parte de BS 7799, la cual está dedicada a la gestión de riesgos de seguridad de la información.

BS7799-3 profundiza en estos aspectos y da directrices sobre evaluación de riesgos, tratamiento de riesgos, toma de decisiones por parte de la Dirección, re-evaluación de riesgos, monitorización y revisión del perfil de riesgo, riesgos de seguridad de la información en el contexto del gobierno corporativo y conformidad con otros estándares y regulaciones sobre el riesgo.

3.3.2 Orientados a las buenas prácticas

Todos los estándares han sido resultado de la experiencia que se ha tenido en las instituciones u organismos dando paso a mejoras prácticas (buenas prácticas) las cuales son una compilación de términos o teorías que han llevado a la práctica y han tenido buenos resultados dentro de las corporaciones.
Las organizaciones que utilizan las TI saben que necesitan accionar las buenas prácticas para poder llevar a cabo un proceso de implementación adecuado y de esta manera no generar riesgos en la información.

Cabe mencionar que las mejores prácticas tienen un ámbito de aplicación universal y son fáciles de entender, pero la implementación resulta muy compleja

3.3.2.1 ISO 27002 (antes 17799:2000)

Como hemos estado estudiando en este capítulo existen diferentes normas y regulaciones tales como *Health Insurance Portability and Accountability Act* (HIPAA), Sarbanes-Oxley, y el Gramm-Leach-Bliley Act (GLBA) que nos demandan tener Seguridad de la Información. La Organización Internacional para la Estandarización (ISO) creó el ISO 27002 el cual nos proporciona un esqueleto para el Sistema de Gestión de la Seguridad de la Información de tal forma que se puede aplicar a cualquier requisito de Seguridad de la Información, y puede ser ajustable a futuros reglamentos y requisitos.

Contiene 39 objetivos de control y 133 controles aplicables (en relación a la gestión de la continuidad de negocio, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, entre otros muchos), agrupados en 11 dominios. Ayudan a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información.

ISO 27002 tuvo su origen en el estándar de seguridad de la información ISO 17799, descendiente del BS 7799. BS 7799 fue publicado en Inglaterra en 1995 y teniendo actualizaciones en 1998 y 1999, sin embargo se requería de un estándar de carácter internacional que permitiera reconocer o validar el

marco de referencia de seguridad aplicado por las organizaciones, es por eso que se elaboró en diciembre del 2000 el estándar ISO17799:2000, el cual está basado principalmente en la primera parte del BS 7799 conocida como Código de Práctica.

Podemos definir a ISO 27002 como un conjunto de prácticas recomendadas (buenas prácticas) a nivel mundial para garantizar la Seguridad de la Información a nivel institucional. Considerada una métrica internacional para determinar niveles y objetivos de Seguridad de la Información a ser alcanzados por las organizaciones, aunque no es de obligatorio cumplimiento, proporciona una base sólida para un programa de seguridad de la información.

Al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, está orientada a la preservación de los atributos de confidencialidad, integridad y disponibilidad de la información.

Lo primero que hace el estándar de seguridad ISO 27002 es identificar por medio de un análisis de riesgos los activos de la información y las amenazas en contra de estos. Con esto se seleccionan los controles que apliquen a la organización para proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

ISO17799:2005, tenía 10 áreas las cuales posteriormente fueron renombradas y reorganizadas, lo que permitió el surgimiento de la ISO-27002 y la cual se agrupa en los siguientes dominios:

1. Políticas de seguridad
2. Organización de la seguridad de la información
3. Gestión de activos
4. Seguridad de los recursos humanos
5. Seguridad física y ambiental
6. Gestión de comunicaciones y operaciones
7. Control de acceso
8. Sistemas de información; adquisición, desarrollo y mantenimiento
9. Gestión de incidentes de seguridad de la información
10. Gestión de la continuidad del negocio
11. Conformidad

3.3.2.2 COBIT

El modelo COBIT (por sus siglas en inglés *Control Objectives for Information and related Technology*) proporciona buenas prácticas por medio de un marco referencial de dominios y procesos, proveyendo guías detalladas sobre objetivos de control para los procesos de gestión de tecnología de información. Surge en el ámbito de la Auditoria de Sistemas y esta principalmente orientado al control de las actividades, cubriendo todo lo relacionado con los sistemas y tecnologías de la información. Este modelo complementa a los modelos más generales como COSO (EEUU), CoCo (Canadá) o Cadbury (Inglaterra).

Los objetivos principales de COBIT es investigar, desarrollar, publicar y promover un conjunto de Objetivos de Control de TI internacionales, actualizados para ser usado por los Gerentes de Negocios y Auditores.

COBIT ha sido diseñado para ser utilizado por 3 distintos niveles:

- **Gerentes:** Para ayudar a medir el riesgo y controlar la inversión en un ambiente de TI frecuentemente impredecible.
- **Usuarios:** Para otorgarles confianza respecto a la seguridad y los controles que se aplican en los servicios de TI. Hay una creciente necesidad de los usuarios por contar con niveles adecuados de control y seguridad.
- **Auditores:** Para sustentar sus opiniones y/o asesorar a la Gerencia respecto a los controles necesarios.

Para lograr los objetivos institucionales, la información necesita satisfacer algunos criterios de información, llamados por COBIT como requerimientos los cuáles se clasifican en tres grupos:

- **Requerimientos de Calidad:** Calidad, costo, entrega.
- **Requerimientos Fiduciarios:** Eficacia y eficiencia en las operaciones, confiabilidad de la información, Cumplimiento de leyes y regulaciones.
- **Requerimientos de seguridad:** Confidencialidad, integridad, disponibilidad.

COBIT divide TI en 34 procesos pertenecientes a cuatro dominios o recursos TI, los cuáles dan una visión completa de cómo controlar, gestionar y medir un proceso:

1. **Planeación y Organización (PO):** Cubre las estrategias y tácticas para encontrar la forma en que la TI ayude a lograr los objetivos de la organización.
2. **Adquisición e Implementación (AI):** Para realizar las estrategias de TI, se necesita identificar, desarrollar o adquirir soluciones, así como implantarlas e integrarlas a los procesos del negocio.
3. **Entrega y Soporte (ES):** Se preocupa por la entrega de los servicios demandados, que van desde operaciones de seguridad y continuidad hasta entrenamiento de personal.
4. **Monitoreo (M):** Todos los procesos son evaluados para verificar los criterios de calidad y cumplimiento. Vigilando los procesos de control de la organización.

3.3.2.3 ISF-SGP

El estándar de buenas prácticas para la Seguridad de la información (*Standard of Good Practice for Information Security*, ISF-SGP) fue creado para ayudar a las organizaciones de los riesgos asociados a los sistemas de información no importando su estructura o tamaño de ésta. Es una herramienta muy importante para mejorar la calidad y la eficiencia de los controles de seguridad aplicados a la organización.

3.3.2.4 BS 25999

BSI (*British Standards Institution*) publicó en 2006 BS25999-1, el cuál está orientado a las buenas prácticas dedicado a la gestión de la continuidad de negocio. Puede ser utilizado por cualquier organización grande, mediana o pequeña, tanto del sector público como privado.

Hoy en día las entidades necesitan disponer de planes de continuidad de negocio que minimicen la inactividad de la organización en caso de cualquier tipo de interrupción.

Teniendo su origen en PAS 56:2003, establece el proceso por el cual una organización puede desarrollar e implementar la continuidad de negocio, incluyendo una completa lista de controles basada en las mejores prácticas de BCM (*Business Continuity Management*).

BS 25999-2 establece los requisitos para el establecimiento, implementación, operación, monitorización, revisión, ejecución, mantenimiento y mejora del Sistema de Gestión de Continuidad de Negocio

3.3.3 Orientado a procesos

En la actualidad las organizaciones se encuentran en una continua competencia con otras, buscando tener éxito y alcanzar buenos resultados u objetivos preestablecidos. Para esto es necesario gestionar sus actividades y recursos con la finalidad de orientarlos hacia la consecución de esos objetivos. Para esto se utilizan diferentes modelos reconocidos para establecer, documentar y mantener sistemas de gestión que les permitan dirigir y controlar sus respectivas organizaciones.

Existen diferentes modelos orientados a los procesos de los mas nombrados y mencionados en este capítulo son el ISM3, ISO 9001, BS 7799-2:2002, CMMI y ITIL, cuyo objetivo es implantar un sistema de gestión dentro de una organización.

Los modelos orientados a procesos son aquellos que realizan un esquema general de procesos y procedimientos para garantizar que la organización realiza todas las tareas necesarias paras alcanzar sus objetivos previamente establecidos.

La visión orientada a procesos exige que la organización defina de manera sistemática las actividades que componen un proceso, identifique la interrelación entre los mismos, defina al responsable del mismo (gestor de su funcionamiento), introduzca criterios (indicadores) para medir los resultados de capacidad y eficacia del mismo, y como consecuencia de esto último introducir criterios que permitan la mejora del mismo.

3.3.3.1 Modelo de Madurez de la Gestión de la Seguridad de la Información (ISM3)

El Modelo de Madurez de la Gestión de la Seguridad de la Información (ISMMM o ISM3, del inglés *Information Security Management Maturity Model*) es un estándar abierto creado por Vicente Aceituno y publicado bajo la licencia Creative Commons.

El propósito de los sistemas de gestión de seguridad (ISM) es prevenir o mitigar los ataques, errores y accidentes que puedan poner en riesgo la seguridad de los sistemas de información y los procesos organizativos soportados por ellos. Una de las principales ventajas de ISM es que los Accionistas y Directores pueden ver con mayor facilidad la Seguridad de la Información como una inversión, dado que es mucho más sencillo medir su rentabilidad y comprender su utilidad.

ISM3 pretende cubrir la necesidad de un estándar simple y aplicable de calidad para sistemas de gestión de la seguridad de la información. Proporciona un marco para ISM que puede utilizarse para todo tipo de organizaciones; desde las pequeñas que realizan sus primeros esfuerzos, hasta un nivel alto de sofisticación por grandes organizaciones como parte de sus procesos de seguridad de la información. Los sistemas de gestión basados en ISM3 pueden certificarse bajo ISO9001 o ISO27001.También cuenta con un proceso de certificación que permite a una organización autoevaluar su madurez, o bien obtener una certificación de un auditor independiente.

Un factor importante para la adopción de ISM3 es que el estándar contempla la protección de inversión realizada en sistemas de manejo de la seguridad de la información y en prácticas y políticas propias de la organización, incorporando éstas en el análisis y puesta en marcha de los procesos necesarios para satisfacer los requerimientos del modelo.

ISM3 cuenta con 5 Niveles de Madurez los cuales se adaptan a los objetivos de seguridad de la organización y a los recursos que están disponibles; el Nivel 1 implica baja inversión, metas bajas de seguridad y riesgos reducidos y el Nivel 4 implica mucha inversión, altas metas de seguridad y riesgos bastante reducidos. Para obtener la certificación en alguno de estos niveles de seguridad es necesario formalizar una documentación con los procedimientos de seguridad, un encargado de supervisar, y el demostrar que los procedimientos son realizables, tanto a nivel de infraestructura como de contar con el personal calificado.

La mayoría de organizaciones no necesitan una certificación ISM-4, que es adecuada para sistemas de nivel crítico como empresas financieras o de servicios vitales; la gran mayoría de las organizaciones encuentran suficiente los niveles ISM-1 o ISM-2.

3.3.3.2 ISO 9001:2000

En el año 2000 surgió la versión de ISO 9001:2000 dejando obsoletas ISO 9002 y 9003 del año 1994. Es una norma de la Organización Internacional para la Estandarización, la única norma de la familia ISO 9001 certificable.

Ésta norma específica los requisitos para un sistema de gestión de la calidad, que puede ser utilizado por una organización para demostrar su capacidad de satisfacer los requisitos del cliente.

Es norma internacional, genérica e independiente de cualquier industria o sector económico, y es aplicable a todos los tipos y tamaños de empresas, así como en el caso de que la empresa sea de productos y/o servicios. Es decir, ISO 9001 propone principios para mejorar la calidad final del producto mediante sencillas mejoras en la organización de la empresa. Las mejoras, causan un beneficio en la calidad final del producto, y de la satisfacción del consumidor, que es lo que pretende quien adopta la norma como guía de desarrollo empresarial.

La norma está basada en un modelo de proceso y desarrolla los 8 principios de la Gestión de Calidad, elaborados por ISO que actúan como base y fundamento de las normativas relacionadas con la Gestión de la Calidad., los cuáles son:

- Principio 1: Organización centrada en el cliente
- Principio 2: Liderazgo
- Principio 3: Compromiso de las personas
- Principio 4: Enfoque a procesos
- Principio 5: Enfoque hacia la Gestión del Sistema
- Principio 6: Mejora Continua
- Principio 7: Enfoque objetivo para la toma de decisiones
- Principio 8: Relaciones con el suministrador mutuamente beneficiosas

Estos principios básicos de la gestión de la calidad, son reglas de carácter social encaminadas a mejorar la marcha y funcionamiento de una organización mediante la mejora de sus relaciones internas.

ISO 9001:2000 consiste en una introducción y contiene 8 cláusulas:

1. Ámbito
2. Referencias normativas
3. Términos y condiciones
4. Sistema de Gestión de Calidad
5. Responsabilidades de la Dirección
6. Gestión de los Recursos
7. Realización del producto
8. Medición, análisis y mejora

Las cláusulas 4 a 8 constituyen la base del Sistema de Gestión de Calidad documentado, las cuáles reflejan el ciclo de Deming "Planificar, Hacer, Comprobar, y Actuar", bien conocido en el mundo de la calidad.

3.3.3.3 BS 7799-2:2002

En 1901 BSI (*British Standards Institution*) fue la primera entidad de normalización con reconocimiento a nivel mundial para los sectores públicos y privado, responsable de importantes normas como fueron BS 5750 (ISO 9000), BS 7750 (ISO 14001).

Se divide en dos partes, la primera parte (BS7799-1) es una guía de buenas prácticas, para la que no se establece un modelo de certificación y la segunda (BS7799-2) es la que se audita y certifica en aquellas empresas solicitantes que hayan desarrollado un Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI, es un enfoque sistémico para gestionar, información sensible en la organización, para que este segura.

BS7799-2, es una guía de auditoría del SGSI basada en los requisitos que deben ser cubiertos por la organización. Contiene especificaciones para certificar los dominios individuales de seguridad para poder registrarse a esta norma.

El BS 7799-2:2002 es una metodología estructurada y reconocida internacionalmente para evaluar, implementar y administrar la seguridad de la información; la cuál es evaluable y certificable. Plantea los requerimientos para un Sistema de Gestión de la Información en la organización. Ayuda de manera sistemática a identificar, gestionar y minimizar el rango de amenazas a la cual la información regularmente esta sujeta. Requiere de un acercamiento sistemático para la evaluación de riesgo, incluyendo el desarrollo de un plan de tratamiento de riesgo para relacionar el riesgo a la confidencialidad, integridad y disponibilidad; establecer objetivos para reducir el riesgo a un nivel aceptable; determinar el criterio para aceptar el riesgo; y evaluar las opciones de tratamiento de riesgos. El proceso engloba, personas, procesos y sistemas de tecnología de información.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.
La ISO 27001 es un estándar certificable publicado el 15 de octubre del 2005, su origen está en la BS 7799-2:2002 es por eso que explicaremos a detalle este estándar. Es la norma principal de la serie 27000 y contiene los requisitos del sistema de gestión de seguridad de la información. Proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Está basado como otros en PDCA (Plan-Do-Check-Act; o

ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

ISO 27001 aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua.

ISO27001 ayuda a considerar y adoptar los controles necesarios en los procesos de negocio y tratamiento de la información para satisfacer las demandas de la empresa, legales y de los clientes en materia de seguridad de la información.

3.3.3.4 Modelo de Capacidad y Madurez Integrado (CMMI)

El Modelo de Capacidad y Madurez Integrado (*Capability Maturity Model Integration*, CMMI) es una fusión de modelos de mejora de procesos para ingeniería de sistemas, ingeniería del software, desarrollo de productos integrados y adquisición del software. Su primera versión fue publicada en enero del 2002, desarrollado por el Instituto de Ingeniería del Software de la Universidad *Carnegie Mellon* (*Software Engineering Institute, SEI*), enfocándose inicialmente hacia los procesos relativos al desarrollo de software, aunque posteriormente se extendió hacia otras temáticas organizacionales (dominios o disciplinas), como la gestión del talento humano y el desarrollo de proyectos. Desde entonces ha sido uno de los modelos más utilizados en la industria del software.

Se dice que es un modelo descriptivo que detalla los atributos esenciales que deberían caracterizar a una organización en un determinado nivel de maduración. Es normativo donde las prácticas detalladas caracterizan los tipos normales de comportamiento esperables en una organización que ejecuta proyectos a gran escala. La mejora continua de los procesos se basa en muchos pasos pequeños y evolutivos en vez de innovaciones revolucionarias.
Sus principales características son el disminuir o eliminar la redundancia en el trabajo, aumentar la fiabilidad en la predicción de costos, aumentar el rehúso de productos y procesos, y disminuir costos debido a través de la evaluación y mejora continua de los procesos.

Proporciona objetivos cuantificables y las valoraciones están orientadas a determinar si se alcanza un determinado nivel de madurez en el proceso.

CMMI al ser un modelo de calidad del software, clasifica a las organizaciones en niveles de madurez y así conocer la madurez de los procesos que se realizan para producir software.

Cada nivel comprende un conjunto de objetivos que, una vez alcanzados, estabilizan un componente importante del proceso de software. Al alcanzar cada nivel del marco de madurez se establece un componente diferente en el proceso de software, resultando en un incremento en la capacidad de proceso de la organización. Los niveles de madurez son: Initial, Managed, Defined, Quantitatively Managed & Optimizing.

3.3.3.5 Biblioteca de Infraestructura de Tecnologías de la Información (ITIL)

Biblioteca de Infraestructura de Tecnologías de la Información (*Information Technology Infraestructure Library*, ITIL) surgió durante los años 80 en el Reino Unido como un modelo orientado a la gestión de las operaciones y servicios de los sistemas y tecnologías de la información y comunicación (*Information and Communications technology Systems* - ICT), siendo el más aceptado mundialmente. Constaba de 10

libros centrales cubriendo las áreas de Soporte del Servicio y Prestación del Servicio. Después fueron soportados por 30 libros complementarios que cubrían otras áreas que iban desde el cableado hasta la gestión de continuidad del negocio. En el año 2000 se hizo una revisión para reestructurar y se hiciera más fácil acceder a la información para administrar los servicios.

ITIL nació de un conjunto de publicaciones de las mejores prácticas para la Gestión de Servicios de TI integradas bajo el enfoque de procesos, los cuales están orientados a la administración de la infraestructura de los servicios que la organización requiera de TI, a través de una amplia lista de roles, tareas, procedimientos y responsabilidades que pueden adaptarse a cualquier organización de TI dependiendo de las necesidades, circunstancias y experiencia. Está específicamente desarrollada para los servicios de mantenimiento y operación de TI, y proporciona objetivos de servicio además de actividades e indicadores clave de servicio. Nos presenta un modelo muy completo el cuál documenta las técnicas, herramientas y considera el factor tecnología como algo a valorar dentro de sus esquema, además de detallar el conjunto mínimo de roles necesarios para el desarrollo con garantías de los procesos.

Características de ITIL

La forma más fácil y rápida de definir ITIL es la siguiente:

- Es un marco de trabajo de procesos IT no propietario.
- Es independiente de los proveedores.
- Es independiente de la tecnología.
- Está basado en los resultados de las mejores prácticas.

ITIL provee:

- Terminología estándar.
- Interdependencias entre los procesos.
- Lineamientos para la implementación.
- Lineamientos para la definición de roles y responsabilidades de los procesos.
- Lista de chequeo de madurez.
- ¿Qué hacer? y ¿qué no hacer?.

3.3.4 Orientado a controles

Existen algunos estándares que están orientados a controles los cuáles se explicarán brevemente tomando en cuenta que son fáciles de auditar y aparentemente garantiza resultados, pero tienen la desventaja de que son muy complejos para ser implementados y pueden resultar muy poco flexibles.

3.3.4.1 ISO 13335-4

Éste estándar esta dirigido a proporcionar guías sobre la manera de administrar la seguridad de las TI. Se dirige a los responsables de administrar la seguridad, los cuáles pueden aplicar ésta guía para las diferentes áreas de trabajo.

Los principales objetivos de este estándar son:

- Definir y describir los conceptos asociados con Seguridad de TI.

- Identificar las relaciones que deben existir entre la administración de seguridad en TI con la administración general de TI.
- Presentar modelos definidos para analizar e implementar una estructura adecuada de seguridad en TI.
- Proveer una guía general de referencia para evaluar e implementar la seguridad de TI.

El ISO 13335 está compuesto de:

- **Parte 1:** Conceptos y Modelos de Seguridad en TI. La cuál provee los conceptos fundamentales y modelos para describir la administración de seguridad en TI. **Parte 2:** Planificación y Administración de la Seguridad de TI. Diseñado para los gerentes responsables de sistemas de TI.
- **Parte 3:** Técnicas de Administración de Seguridad de TI. Describe técnicas orientadas al personal involucrado con actividades de administración y gerencia durante el ciclo de vida del proyecto como son la planificación, diseño, implementación, testeo, adquisición u operación.
- **Parte 4:** Selección de controles. Provee guías para la selección de controles, las cuáles pueden ser soportadas con el uso de un modelo básico y los respectivos controles.
- **Parte 5:** Guías de Administración para Seguridad de redes. Provee guías sobre las redes y comunicaciones para aquellos responsables por su seguridad.

3.3.4.2 COSO

El modelo COSO (*Committee of Sponsoring Organizations* de la *Treadway Commission*, Comité de Organizaciones Patrocinantes de la Comisión Treadway) tuvo sus inicios en 1985, su finalidad es identificar los factores que causan informes financieros fraudulentos y emitir las recomendaciones que garantizasen la máxima transparencia informativa en tal sentido.
COSO ha establecido una definición común de controles internos, normas y criterios contra los cuales las empresas y organizaciones pueden evaluar sus sistemas de control.

El informe COSO consiguió que cuando se plantea una discusión o problema de control interno, tanto a nivel práctico de las empresas como a nivel de auditoría interna y externa, o a los niveles académicos y legislativos, los interlocutores tengan una referencia conceptual común.

Existe una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La relación se representa con una matriz tridimensional, en forma de cubo.

COSO define al Control Interno como un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de una entidad, diseñado con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y Eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las Leyes y normas aplicables.

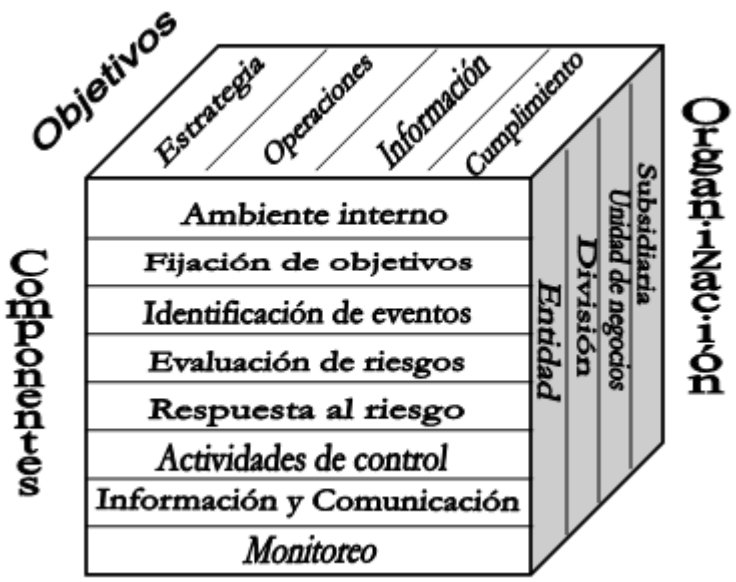


Figura 3.10 Modelo COSO

Las cuatro categorías de objetivos (estrategia, operaciones, información y conformidad) están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo.

3.3.5 Orientados a productos

Existen estándares dedicados a la evaluación de las características de seguridad y capacidad, de los productos de tecnología de la información y sistemas.

Los estándares orientados a productos proporcionan un conjunto común de estándares que los usuarios con operaciones internacionales pueden utilizar para escoger productos que se ajusten localmente a sus necesidades de seguridad. Estos estándares proporcionan unos medios y mecanismos objetivos que permitirán tomar decisiones en base a algo más sólido que las meras percepciones.

3.3.5.1 Criterios Comunes

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad bajo el nombre de TCSEC (*Trusted Computer System Evaluation Criteria*) mejor conocido como el "libro naranja". Posteriormente varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas más flexibles y adaptables a la constante evolución de los sistemas de TI.

En 1991 la comisión europea (Francia, Alemania, Holanda y el Reino Unido) publicó el ITSEC *(Information Technology Security Evaluation Criteria*). En Canadá, igualmente desarrollaron en 1993 los criterios CTCPEC (*Canadian Trusted Computer Product Evaluation*) uniendo los criterios americanos y europeos. Ese mismo año el Gobierno americano publicó los Federal Criteria como una aproximación a unificar los criterios europeos y americanos.

Al notar todos estos estándares, se toma la decisión de crear uno internacional por lo que la ISO (International Organization for Standardization) y la IEC (the International Electrotechnical Commission) comienzan a trabajar a principios de las 90´s con la certificación Common Criteria (o ISO-IEC 15408).

Al final esta norma combina los mejores elementos del ITSEC, la CTCPEC (de Canadá) y el Criterio Federal Norteamericano (FC), en el cual participaron 14 países para alinear y desarrollar un criterio de evaluación de seguridad.

Los Criterios Comunes (Common Criteria), mejor conocido como la norma ISO 15408, componen el estándar internacional cuyo propósito es identificar y evaluar la seguridad de los productos o sistemas de Tecnologías de la Información.

Los objetivos de la ISO 15408, son:

- Definir un criterio común para la especificación del nivel de seguridad de sistemas y productos de Tecnología de Información (TI) de diverso tipo.
- Definir un conjunto de requerimientos común para las funciones de seguridad de productos del área.
- Permite efectuar análisis de evaluaciones de seguridad independientes (distintos objetos de TI)
- Proporcionar una guía para el desarrollo de productos o sistemas de TI con funciones de seguridad.
- Contar con una guía para la adquisición y configuración de productos de tecnología y seguridad.

CAPÍTULO 4

MODELO DE MADUREZ EN LA ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA (ISM3)

El Modelo de Madurez de Gestión de la Seguridad de la Información (ISMMM o ISM3, del inglés *Information Security Management Maturity Model*) tiene como propósito prevenir o mitigar los ataques, errores y accidentes que puedan poner en riesgo la seguridad de los sistemas de información y los procesos organizativos soportados por ellos.

Es importante destacar que está diseñado para ser utilizado en cualquier tipo de organización independientemente de su tamaño.

ISM3 define la madurez en términos de procesos. Se utilizan cuatro modelos conceptuales:

- El Modelo de Gestión de la Seguridad de Información: proporciona un marco para identificar los procesos principales en un sistema ISM y evaluar su madurez.
- El Modelo Organizativo: proporciona una visión basada en responsabilidades de una organización.
- El Modelo de Sistema de Información: proporciona una manera de describir los componentes principales de los sistemas de información.
- Modelo de Seguridad Contextual: permite a una organización preparar su propia definición de seguridad ajustada al ambiente y misión de la organización.

La notación usada por los procesos ISM3 describe ciertas propiedades fundamentales.

Éstas incluyen:

- El nivel de la organización responsable de cada conjunto de procesos (estratégico, táctico u operativo).
- La fundamentación del proceso. Cada organización tiene un contexto y recursos diferentes, por consiguiente se usan diferentes procesos. Cuando se audita la madurez de los sistemas ISM, tanto la presencia como ausencia de los procesos debe ser justificada.
- Entradas a los procesos.

- Productos de los procesos. Estos pueden ser documentos, como políticas y reportes, o ser el resultado de eventos recurrentes, como realizar un respaldo o analizar archivos de registro.

Debe destacarse que un proceso puede ocurrir en varios lugares diferentes en una organización, controlados por diferentes personas. Cuando esto ocurre, cada instancia del proceso necesita ser evaluada. Los procesos son descritos a alto nivel en la tabla siguiente:

Proceso	**Código y denominación del proceso**
Descripción	La actividad realizada por el proceso.
Fundamentación	Cómo contribuye el proceso a los objetivos específicos y globales.
Documentación	Políticas, Procedimientos y Plantillas de Definiciones de Procesos que necesitan ser descritas o realizadas por el proceso.
Entradas	Entradas al proceso. Las entradas en *cursiva* pueden obtenerse de fuentes que no tienen por qué ser documentos.
Productos de Trabajo	Resultados del proceso. Los productos de trabajo en *cursiva* son productos distintos de documentos.
Propietario del Proceso	Un ejemplo de Propietario del Proceso se da en esta fila. Cada proceso debería tener un y sólo un Propietario del Proceso. Cuando un grupo de personas, como gestores de servicios, son referidos como un Propietario del Proceso, esto significa que cada uno de ellos es responsable de una instancia separada del proceso.
Procesos relacionados	Otros procesos ISM3 que son necesarios para generar las entradas clave.
Metodologías relacionadas	Metodologías y mejores prácticas bien conocidas. Estas metodologías pueden ser útiles para identificar actividades relevantes, riesgos y controles.

Tabla 5.1 Descripción de los procesos a alto nivel

Los siguientes roles son de especial importancia en ISM3 y los estaremos utilizando más adelante:

- *Cliente:* como en la definición ITIL de un cliente, este es un rol que proporciona recursos y conjunto de requerimientos para un proceso y su Propietario de proceso.
- *Gestión estratégica:* un gestor actuando en un rol estratégico.
- *Gestión táctica:* un gestor actuando en un rol táctico.
- *Gestión operativa:* un gestor actuando en un rol operativo.

4.1 Uso de ISM3

El ISM3 puede ser utilizado para el diseño de un ISM apropiado al ambiente y circunstancias particulares de una organización, o para evaluar la madurez de un sistema ISM existente. Sea cual fuese el modo de uso, la selección de los procesos ISM es flexible, dado que cada nivel de madurez requiere cierto conjunto de procesos.

4.1.1 Descripción de niveles

Dentro del ISM3 existen diferentes niveles los cuales pretenden describir sistemas ISM consistentes y prácticos, con distintos niveles de madurez y sofisticación.

Cuando una organización decide adoptar un determinado nivel se recomienda que no restrinja el sistema ISM a procesos obligatorios para un determinado nivel, sino que implemente procesos apropiados para su propio ambiente.

Todos los procesos se asignan en niveles de madurez para mostrar el espectro de desarrollo, desde un sistema ISM básico a uno avanzado. El ISM básico está basado en principios de gestión de calidad y por consiguiente demanda una inversión inicial en procesos de calidad, como la definición de requerimientos de seguridad y documentación.

A continuación se explican brevemente cada uno de los niveles de madurez que tiene el ISM3:

Nivel ISM3 0 (cero): Este nivel puede producir resultados favorables a corto plazo, pero es poco improbable que resulte en una reducción significativa del riesgo de amenazas técnicas e internas de medio a largo plazo sin inversiones impredecibles. Por lo tanto no se recomienda este nivel.

Nivel ISM3 1: Debe resultar en este nivel una reducción significativa del riesgo de amenazas técnicas, con una inversión mínima en procesos ISM esenciales. Este nivel se recomienda para organizaciones con Metas de Seguridad bajas en ambientes de riesgo bajo.

Nivel ISM3 2: Este nivel debería resultar en una mayor reducción del riesgo por amenazas técnicas, con una inversión moderada en procesos ISM. Se recomienda este nivel para organizaciones con Metas de Seguridad normales en ambientes de riesgo normal.

Nivel ISM3 3: El nivel 3 resulta una reducción del riesgo alta por amenazas técnicas, con una inversión seria en procesos ISM. Es recomendado para organizaciones con Metas de Seguridad altas en ambientes de riesgo normal o alto.

Nivel ISM3 4: El último nivel debería resultar en la mayor reducción de amenazas tanto técnicas como internas, por una inversión seria en procesos ISM. Se recomienda a organizaciones afectadas por requerimientos específicos (como suministradoras de energía y agua, instituciones financieras y organizaciones que comparten o almacenan información sensible) con Metas de Seguridad muy altas en ambientes de riesgo normal o alto.

4.1.2 Certificación

El ISM3 puede certificarse asegurando que los procesos ISM cumplen con un estándar mínimo de calidad definido. La certificación está basada en evidencias y cada proceso se califica como *aprobado* si cumple con los siguientes criterios:

- **Documentado**: La documentación debe describir por completo el proceso e incluir plantillas y muestras de los productos del trabajo.
- **Supervisado**: Se requiere evidencia de que cada proceso tiene un Propietario del Proceso competente. Además, se requiere evidencia de que se reportan al Cliente la eficiencia y/o desempeño del proceso.
- **Aprovisionado**: Se requiere evidencia de que hay recursos adecuados en términos de presupuesto, personal y espacio para realizar el proceso. La Evidencia de que un proceso se lleva a cabo es suficiente para probar que está adecuadamente aprovisionado.

4.1.3 Tabla de evaluación

Sobre los criterios anteriores podemos decir que si se aprueba la parte de "Documentado" se requiere producir todos los documentos descritos para un proceso en particular. Si el nombre de un documento no coincide con uno de ISM3, se necesita presentar referencias explícitas a su equivalencia en ISM3 en el documento.

Para obtener un "Sí de aprobado" en Supervisado, debe haber evidencia en el proceso de documentación del nombre del rol o equipo que es el Propietario del Proceso y el nombre del rol o el equipo del Cliente del proceso. También debe haber evidencia documental del informe de desempeño entre el Propietario del Proceso y el Cliente del proceso.

Por último para la aprobación de Aprovisionado, se requiere mostrar que hay recursos adecuados de personal, presupuesto e instrumentos técnicos para realizar el proceso. Como alternativa, los productos del trabajo pueden demostrar indirectamente que el proceso está adecuadamente aprovisionado.

Para aprobar un Proceso, todos los criterios deben haber sido evidenciados.

Se lleva a cabo un análisis de aprobación utilizando la siguiente tabla:

	Documentado	**Supervisado**	**Aprovisionado**	**Puntaje Global**
GP-1 Gestión de Documentación				

Tabla 5.2 Tabla de Evaluación General

La tabla se divide en 3 columnas de criterio (Documentado, Supervisado, y Aprovisionado) las cuáles se puntualizan de la siguiente manera:

- Sí: 1
- No: 0
- Incompleto: 0.5
- Se desconoce: -1

Posteriormente se calcula el puntaje promedio de un proceso el cuál se registra en la última columna de la tabla llamada Puntaje Global que es la suma de las 3 columnas de criterio. Para que un proceso obtenga un Aprobado, éste debe obtener 3 puntos, si no, obtiene un Desaprobado.
Para aprobar un nivel de madurez, se requiere un puntaje promedio de 3,0 en los Procesos recomendados. Si las razones de omitir un Proceso recomendado están explicadas en la Política de Seguridad, éste puede ser excluido del puntaje promedio global (No aplicable).

Igualmente, los procesos por encima del nivel de madurez valorado son excluidos. Algunas organizaciones tienen varias instancias de los Procesos.

4.1.4 Tabla de niveles

Como ya hemos mencionado ISM3 tiene cinco niveles de maduración que van del Nivel 0 hasta el Nivel 4. Cada nivel de madurez es atado a los objetivos de seguridad de la organización por lo que el nivel de madurez depende del tamaño de la organización y los requerimientos de sus servicios.

Para obtener algún nivel es necesario tener cierta documentación de los procesos, los cuáles deben ser revisados y aprobados. Estos documentos serán explicados posteriormente con todos los requisitos que necesita cada uno.

Los documentos para cada uno de los niveles son expuestos en las tablas posteriores.

	Nivel ISM3 0	**Nivel ISM3 1**	**Nivel ISM3 2**	**Nivel ISM3 3**	**Nivel ISM3 4**
GP-1 Gestionar la documentación		●	▲	■	♦

Tabla 5.3 General

	Nivel ISM3 0	**Nivel ISM3 1**	**Nivel ISM3 2**	**Nivel ISM3 3**	**Nivel ISM3 4**
SSP-1 Informar a las autoridades		●	▲	■	♦
SSP-2 Coordinar		●	▲	■	♦
SSP-3 Alcanzar visión estratégica		●	▲	■	♦
SSP-4 Definir las reglas para la separación de responsabilidades: transparencia, particionado, supervisión, rotación y separación de responsabilidades (TPSRSR).					♦

SSP-5 Comprobar el cumplimiento con las reglas TPSRSR.					♦
SSP-6 Asignar recursos para seguridad de la información		●	▲	■	♦

Tabla 5.4 Gestión Estratégica

	Nivel ISM3 0	**Nivel ISM3 1**	**Nivel ISM3 2**	**Nivel ISM3 3**	**Nivel ISM3 4**
TSP-1 Informar a la gestión estratégica.		●	▲	■	♦
TSP-2 Gestionar los recursos asignados.		●	▲	■	♦
TSP-3 Definir las Metas de Seguridad.		●	▲	■	♦
TSP-4 Definir los indicadores para los procesos de seguridad.				■	♦
TSP-5 Definir grupos de propiedades.			▲	■	♦
TSP-6 Definir ambientes y ciclos de vida.			▲	■	♦
TSP-7 Investigar antecedentes y referencias					♦
TSP-8 Seleccionar el personal de seguridad.					♦
TSP-9 Capacitar al personal de seguridad.				■	♦

TSP-10 Definir procesos disciplinarios.			▲	■	♦
TSP-11 alcanzar conciencia en Seguridad.			▲	■	♦
TSP-12 Seleccionar procesos específicos.		●	▲	■	♦

Tabla 5.5 Gestión Táctica

	Nivel ISM3 0	**Nivel ISM3 1**	**Nivel ISM3 2**	**Nivel ISM3 3**	**Nivel ISM3 4**
OSP-1 Informar a la gestión táctica.		●	▲	■	♦
OSP-2 Seleccionar las herramientas para implementar las medidas de seguridad.			▲	■	♦
OSP-3 Gestionar el inventario.				■	♦
OSP-4 Controlar el cambio del ambiente de los sistemas de información.			▲	■	♦
OSP-5 Refaccionar del ambiente.		●	▲	■	♦
OSP-6 Limpiar el ambiente.			▲	■	♦
OSP-7 Fortalecer el ambiente.			▲	■	♦
OSP-8 Controlar el ciclo de vida del desarrollo de software.				■	♦

OSP-9 Controlar los cambios en las medidas de seguridad.			▲	■	♦
OSP-10 Gestionar el respaldo y redundancia.		●	▲	■	♦
OSP-11 Controlar el acceso a servicios, canales de repositorios e interfaces.			▲	■	♦
OSP-12 Llevar el registro de usuarios.			▲	■	♦
OSP-13 Gestionar el cifrado.				■	♦
OSP-14 Gestionar la protección del ambiente físico.			▲	■	♦
OSP-15 Gestionar la continuidad de operaciones.				■	♦
OSP-16 Gestionar el filtrado y segmentación.		●	▲	■	♦
OSP-17 Gestionar la protección Contra Malware		●	▲	■	♦
OSP-18 Gestionar el aseguramiento.					♦
OSP-19 Emular ataques, errores y accidentes.			▲	■	♦
OSP-20 Emular incidentes.				■	♦

OSP-21 Comprobar la calidad de la Información.					♦
OSP-22 Monitorizar alertas.			▲	■	♦
OSP-23 Detectar y analizar los eventos.					♦
OSP-24 Manejar los incidentes y pseudo-incidentes.				■	♦
OSP-25 Realizar el análisis forense.					♦

Tabla 5.6 Gestión Operativa

Como podemos ver la primera columna contiene el nombre de los documentos y las cinco columnas restantes son los niveles de madurez con los documentos que necesitan ser aprobados para ese nivel. Para diferenciar cada uno de los niveles se les asignó los siguientes signos:

Nivel 1: ●

Nivel 2: ▲

Nivel 3: ■

Nivel 4: ♦

4.2 Modelo de Gestión de la seguridad de la información

En este modelo se plantea que la seguridad es el resultado de un proceso, es decir, mientras mejor sean los procesos de gestión de la seguridad, mayor protección se obtendrá de los recursos disponibles. ISM3 no considera ningún conjunto único de medidas de seguridad o procesos de gestión de seguridad como obligatorio o útil para todas las organizaciones.

Cuando hablamos de gestionar algo significa definir y alcanzar metas, optimizando al mismo tiempo el uso de recursos. Las actividades de gestión incluyen habitualmente la planificación, dirección, control y coordinación.

Hay tres niveles de Gestión de Seguridad:

- Estratégico, que trata de los objetivos globales y la provisión de recursos.
- Táctico, el cual trata de los objetivos específicos y la gestión de recursos.
- Operativo, el cual trata del logro de los objetivos definidos.

Cada uno de los niveles explicados anteriormente tiene asignado diferentes documentos los cuáles se pueden ver en el ANEXO A.
En la aplicación de ISM3, no es importante el grado de gestión, sino la forma de pensar acerca de cada proceso.

4.2.1 Objetivos generales

Los objetivos generales de un sistema ISM son:

- Prevenir y mitigar incidentes que podrían amenazar la propiedad de la organización y la producción de productos y servicios que dependen de los sistemas de información.
- Optimizar el uso de la información, presupuesto, personal, tiempo e infraestructura.

4.2.2 Productos de trabajo generales

Los productos de trabajo del sistema ISM son:

- Mitigación de incidentes.
- Prevención de incidentes.
- Reducción de riesgo.
- Confianza.

Mientras mejor sean los procesos para garantizar estos productos, mayor será la seguridad, y se obtendrá un reiterado cumplimiento de los Objetivos de Seguridad.

Los productos de trabajo pueden incluir indicadores como componentes de un informe. Un indicador es información cualitativa o cuantitativa útil para detectar anomalías significativas y tomar decisiones. Los indicadores de eficacia miden el éxito de un proceso comparándolo con sus requerimientos. Los indicadores de eficiencia miden el éxito de un proceso comparándolo con los recursos utilizados. Los indicadores están basados en información, la cual a su vez está basada en datos. La diferencia entre datos e información es que la información tiene contexto.

4.2.3 Práctica genérica: Documentación

El proceso de documentación tiene la función de garantizar que el proceso esté definido, sea robusto y repetible. El proceso de Gestión de Documentación soporta esto mediante la definición de documentos de estándares de calidad y ayuda a mantener el sistema ISM actualizado mediante los requerimientos de expiración y revisión de documentos. Este proceso incluye:

- Revisión y procedimientos de aprobación cuando un documento se crea o actualiza.
- Distribución de la versión actual y la revocación de las versiones obsoletas.
- El número y fecha de versión de cada documento.
- Las políticas de retención, expiración y obtención de documentos.

- El mantenimiento del catálogo de documentos.

Todas las descripciones de los procesos relacionados a la Gestión de Documentación podemos encontrarlas en el ANEXO A.

4.2.4 Práctica Específica: Gestión Estratégica

Las autoridades son los Clientes de la gestión estratégica. La gestión estratégica es responsable ante las autoridades para el uso de los recursos a través de los acuerdos establecidos.

La gestión estratégica cumple con las siguientes responsabilidades con respecto a la seguridad:

- Proporcionar liderazgo y coordinación de:
  - Seguridad de la información.
  - Seguridad física.
  - Seguridad del lugar de trabajo (fuera del alcance de ISM3).
  - Interacción con otras unidades organizativas.
- Revisar y mejorar el sistema de gestión de seguridad de la información.
- Definir las relaciones con otras organizaciones.
- Proporcionar recursos para la seguridad de la información.
- Definir Objetivos de Seguridad consistentes con los objetivos de la organización, proteger los intereses de las autoridades.
- Definir el esquema de delegación de la organización.

Todas las descripciones de los procesos relacionados a la Gestión de Estrategia podemos encontrarlas en el ANEXO A.

4.2.5 Práctica Específica: Gestión Táctica

La Gestión Estratégica es el Cliente de la Gestión Táctica con respecto a los Procesos ISM3. La Gestión Táctica es responsable ante la Gestión Estratégica del desempeño del sistema ISM y del uso de recursos.

La Gestión Táctica tiene los siguientes propósitos:

- Proporcionar de retroalimentación a la Gestión Estratégica.
- Definir el ambiente para la Gestión Operativa.
  - Definir las Metas de Seguridad.
  - Definir los indicadores de eficiencia y eficacia.
  - Definir las clases de información, prioridades, durabilidad y grupos de calidad.
  - Definir los ambientes y ciclos de vida.
  - Seleccionar los Procesos apropiados para alcanzar las Metas de Seguridad.

- Gestionar el presupuesto, el personal y otros recursos Asignados para la Seguridad de la Información.

Todas las descripciones de los procesos relacionados a la Gestión Táctica podemos encontrarlas en el ANEXO A.

4.2.5.1 Selección segura de procesos

La selección de los Procesos más apropiados para alcanzar las Metas de Seguridad puede estar basada en distintos tipos de evaluaciones y análisis:

- Evaluación de Riesgo.
- Evaluación de Vulnerabilidad.
- Análisis de Impacto en los Servicios.
- Evaluación de Amenazas.
- Análisis ROSI.

ISM3 no condiciona la preferencia de cualquiera de estas técnicas o de cualquier método en particular para llevarlas a cabo. Algunas organizaciones pueden elegir ahorrarse los recursos para realizar cualquiera de estos análisis, y en su lugar elegir el nivel ISM3 más alto que puedan permitirse.

4.2.6 Práctica Específica: Gestión Operativa

La Gestión Operativa informa al *Chief Information Officer* y al Equipo de gestión Táctico de la Seguridad de la Información.

Tiene los siguientes roles:

- Proporcionar retroalimentación a la Gestión Táctica, incluyendo Informes de Incidentes.
- Identificar y proteger bienes.
- Proteger y dar soporte a los sistemas de información en todo su ciclo de vida.
- Gestionar el ciclo de vida de las medidas de seguridad.
- Aplicar los recursos Asignados eficiente y eficazmente.
- Realizar los Procesos para la prevención, detección y mitigación de incidentes (tanto en tiempo real como después de un incidente).

Todas las descripciones de los procesos relacionados a la Gestión Operativa podemos encontrarlas en el ANEXO A.

4.3 Gestión de responsabilidades

La Gestión de la Seguridad de la Información (ISM) no es diferente a cualquier otro Proceso Organizativo. Por consiguiente se deben seguir las reglas para la transparencia, particionado,

supervisión, rotación y separación de responsabilidades (TPSRSR). A continuación se da una Guía de Mejores Prácticas:

4.3.1 Transparencia

Las responsabilidades y canales de reporte se deben definir, documentar y comunicar claramente.

Además:

- Las autoridades deben tener acceso a los Informes Estratégicos de ISM, según los marquen las leyes, regulaciones y requerimientos de gobierno de la organización.
- Los equipos de gestión ISM estratégicos y tácticos deben tener acceso a los Informes Operativos de ISM.
- Los equipos de gestión ISM estratégicos deben tener acceso a los Informes Tácticos de ISM.

Se recomienda la transparencia en todos los niveles de madurez.

4.3.2 Particionado

Cada instancia de los Procesos ISM debe tener uno y sólo un Propietario del Proceso. El Propietario del Proceso puede delegar un Proceso, pero aun mantiene la responsabilidad por la competencia y la diligencia con que sea realizado.

Se recomienda el particionado en todos los niveles de madurez.

4.3.3 Supervisión

Cada Proceso ISM debe tener al menos un supervisor.

- Las autoridades pueden actuar como supervisores de la visión estratégica del ISM, según los marquen las leyes, regulaciones y requerimientos de gobierno de la organización.
- Los equipos de gestión ISM estratégicos pueden actuar como supervisores de los Procesos ISM tácticos.
- Los equipos de gestión ISM tácticos pueden actuar como supervisores de los Procesos ISM operativos.

Se recomienda el uso de supervisión para los niveles de madurez 3 y superiores.

4.3.4 Rotación

Todos los procesos sensibles, especialmente las auditorías, deben ser transferidos periódicamente a otro Propietario del Proceso competente. No se debería poder predecir quién será el siguiente Propietario del Proceso. Se recomienda la rotación para el nivel de madurez 4.

4.3.5 Separación

Los siguientes roles relacionados deberían mantenerse separados:

Incompatibilidad	Nivel ISM3
Auditor del Proceso & Propietario del Proceso (PO)	1 y superiores
Víctima del Incidente & Investigador Forense	1 y superiores
Denunciante de un Incidente & Investigador Forense	1 y superiores
Auditor ISM3 & y otros PO	1 y superiores
PO Estratégico & PO Operativo (esta incompatibilidad garantiza supervisión)	2 y superiores
Autorizador & Administrador del Sistema	2 y superiores
PO del Control de Acceso Físico & PO del Control de Acceso Lógico	3 y superiores
Personal Requerido & Personal de Selección (para prevenir favoritismo)	3 y superiores
Clasificador de Repositorio & Usuario de Repositorio	3 y superiores
Propietario del Sistema de Información & Administrador del Sistema	3 y superiores
Denunciante de una debilidad & Gestor del parcheo	3 y superiores
Administrador del Sistema & Usuario	3 y superiores
Operador de Resguardo de Repositorio & Bibliotecario de Cintas	4
Administrador de Registros & Mantenedor de Registros	4

Tabla 5.7. Roles Relacionados

4.4 Despliegue

El despliegue de un sistema complaciente con ISM3 depende si existe o no un sistema ISM.

Los pasos en general son:

- Determinar los Requerimientos Regulatorios.
- Determinar los Objetivos de Seguridad de la Información.
- Determinar el Presupuesto de Seguridad de la Información.
- Determinar los ambientes y ciclos de vida.
- Determinar las Metas de Seguridad de la Información.
- Elegir un método de selección de Procesos.
- Nivel de Madurez ISM3.
- Evaluación de Riesgo.
- Evaluación de Vulnerabilidades.
- Evaluación de Impacto en los Servicios.

- Evaluación de Amenazas.
- Evaluación ROSI.
- Seleccionar los Procesos apropiados.
- Revisar las Metas de Seguridad de la Información.
- Determinar los indicadores de Seguridad de la Información.
- Diseñar y documentar el sistema ISM basado en ISM3.
- Acuerdos.
- Políticas.
- Procedimientos.
- Plantillas.
- Implementar el sistema ISM.
- Operar el sistema ISM.
- Auditar o Certificar el sistema ISM periódicamente.
- Mantener y mejorar el sistema ISM.

CAPÍTULO 5

CASO DE ESTUDIO: EVALUACIÓN DE UN PROCESO CRÍTICO CONFORME A LA METODOLOGÍA DEL ISM3

El presente trabajo de tesis fue elaborado para solventar una necesidad muy puntual del Departamento de Seguridad en Cómputo (DSC-FI); el cual pertenece a la Unidad de Servicios de Cómputo Académico (UNICA) de la Facultad de Ingeniería de la UNAM. Dado lo anterior se explica brevemente los fines y propósitos tanto de UNICA como del DSC-FI, y se ejemplifica el uso de ISM3 en uno de los procesos más críticos del Departamento de Seguridad.

5.1 Unidad de Servicios de Cómputo Académico

La Unidad de Servicios de Cómputo Académico es una dependencia de la Secretaría General de la Facultad de Ingeniería de la UNAM, cuya finalidad principal es la de proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad requiere, recursos de cómputo comerciales y de alta especialización que el avance de la educación, el desarrollo de la informática y el ejercicio profesional demanden.

A continuación se muestra el organigrama de la Unidad de Servicios de Cómputo Académico en la figura 5.1.

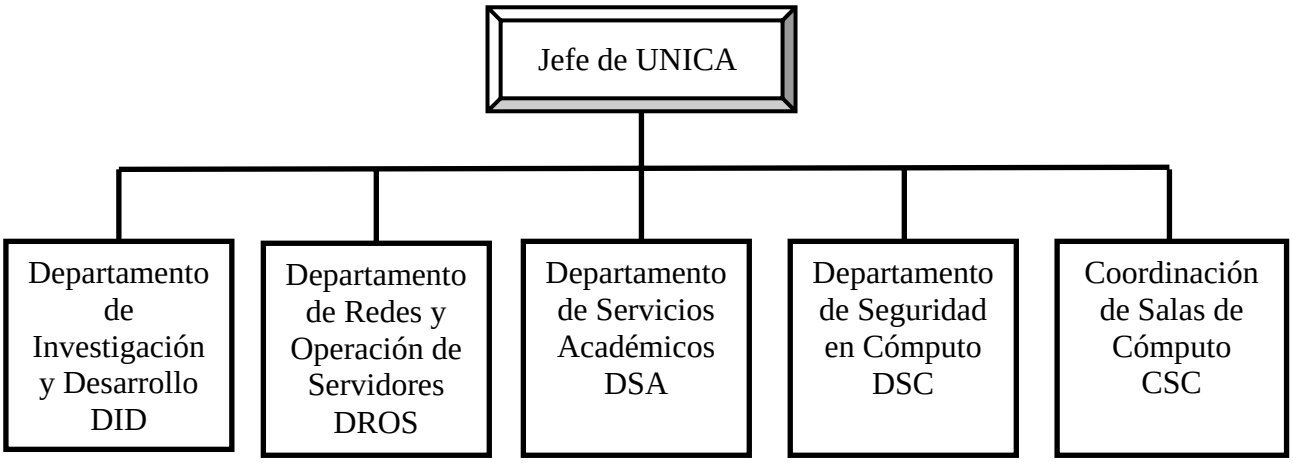


Figura 5.1 Organigrama de la Unidad de Servicios de Cómputo Académico.

5.2 Departamento de Seguridad en Cómputo de la Facultad de Ingeniería

La función del Departamento de Seguridad en Cómputo es instrumentar y administrar la seguridad informática en la Facultad de Ingeniería, el departamento contiene un Plan de Seguridad Informática que permite mitigar los niveles de riesgo dentro de la Facultad.

Sus principales actividades del Departamento de Seguridad en Cómputo son:

- Manejo de Incidentes
    - Proporcionar mecanismos de reporte de incidentes.
    - Entender la amenaza, naturaleza y alcance de los ataques.
    - Identificar nuevos tipos de métodos de ataque.
    - Proporcionar soporte técnico para respuesta de incidentes de seguridad.
    - Facilitar la comunicación entre los sitios y equipos de respuesta.
- Alertas y Anuncios
    - Analizar y desarrollar avisos y anuncios.
    - Retrasmitir avisos de otros equipos.
- Manejo de Vulnerabilidades
    - Analizar y verificar el problema.
    - Coordinarse con otros equipos de respuesta a incidentes y otros expertos de confianza.
    - Mantener la información de las vulnerabilidades en un lugar seguro.
- Sistemas Detectores de Intrusos
    - Revisar las alertas de los sistemas de detección de intrusiones.
    - Actualizar y mantener las firmas de los sistemas detectores de intrusos.

- Revisar y monitorear el ambiente de red existente para establecer una línea base de actividad de la red, con objeto de tener un punto de comparación en contra de potenciales anomalías.
- Mantener registros para usar durante la investigación y recuperación de actividades.

- Educación y Capacitación

  - Crear una cultura de seguridad con cursos de capacitación.
  - Generar documentación que permita a todos los usuarios estar enterados de los avances y actividades actuales de la seguridad en cómputo.
  - Formación de nuevos elementos para la seguridad en los sistemas de cómputo.
  - Capacitación de los elementos del equipo de forma organizada y constante.

- Auditorías

  - Para determinar que tan seguro es un sistema actualmente o que necesita para incrementar su seguridad.
  - Para garantizar que el sistema cumple con los estándares y políticas correspondientes.
  - Para realizar el seguimiento a un incidente de seguridad para determinar qué alteraciones ocurrieron, como ingresaron al sistema, etc.

- Colaboración y Coordinación

  - Colaboración y coordinación con otros equipos de respuesta a incidentes en cómputo y áreas de seguridad.

5.2.1 Misión

La misión del Departamento de Seguridad en Cómputo es proveer un único y confiable punto de contacto para los administradores de redes y servidores de la Facultad de Ingeniería de la UNAM para tratar los problemas de seguridad e incidentes, y a su vez ser el centro más confiable para la recolección y diseminación de información relacionada con las amenazas sobre las redes computacionales, vulnerabilidades y respuesta a incidentes de la Facultad de Ingeniería.

5.2.2 Servicios

El Departamento de Seguridad en Cómputo proporciona servicios a todo el personal de la Facultad de Ingeniería los cuales están listados en orden decreciente conforme a su importancia:

Amenazas e Incidentes de Seguridad en Cómputo

- Amenaza de la seguridad física de seres humanos.
- Ataques a *root*, al sistema o al manejo de la información de cualquier elemento del que se compone la red y que involucre sistemas críticos, multiusuarios y en producción.
- Ataque a la confidencialidad de la información, de las cuentas de usuario, del software, de los sistemas y de la administración en sistemas multiusuarios, críticos y en producción.
- Ataques de denegación de servicios o incidentes relacionados.
- Ataques de cualquier equipo definidos en la constitución hacia equipos externos.

- Ataques a gran escala de cualquiera de este tipo: ataques de *sniffeo*, ingeniería social, *crackeo* de contraseñas, etc.
- Cuentas individuales comprometidas en sistemas críticos, en producción y sistemas multiusuarios.
- Amenazas, hostigamiento y cualquier otro tipo de ofensas que involucren a cuentas de usuario individuales.
- Computadoras personales comprometidas.
- Violación a las políticas de cómputo vigentes.
- Denegación de servicio a cuentas individuales.

5.3 Adopción de ISM3 por el Departamento de Seguridad en Cómputo

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes dentro del Departamento de Seguridad en Cómputo, es por eso que se decidió adoptar un sistema de Gestión de la Seguridad de la Información el cual fuera realizado mediante un proceso sistemático, documentado y conocido por todo el departamento.

Garantizar un nivel de protección total es virtualmente imposible. El propósito de un sistema de gestión de la seguridad de la información en el DSC-FI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

De esta manera es que el DSC-FI ha adoptado al ISM3 como herramienta de gestión para los procesos de seguridad informática. A lo largo de este trabajo de tesis se han mostrado los diferentes aspectos que deben ser cubiertos en una gestión adecuada de las tecnologías de la información y más aún de la seguridad que en ellas se debe de procurar.

Sin embargo los aspectos más fundamentales por los que se ha decidido adoptar al "Modelo de Madurez en la Administración de la Seguridad Informática (ISM3)", es por los siguientes enfoques:

- **Modelo de Gestión de la Seguridad de Información.**

  Es decir proporciona un marco para identificar los procesos principales en un sistema ISM y evaluar su madurez.

- **Modelo Organizativo.**

  Esto significa que proporciona una visión basada en responsabilidades de una organización.

- **Modelo de Sistema de Información.**

  Proporciona una manera de describir los componentes principales de los sistemas de información.

- **Modelo de Seguridad Contextual.**

  Permite a una organización preparar su propia definición de seguridad ajustada al ambiente y misión de la organización.

Como puede observarse, presenta en conjunto un enfoque general sobre el tratamiento de la seguridad, es decir no particulariza en elementos propios de las tecnologías de la información, si no que reconoce

y acepta como parte del proceso de aseguramiento de de redes y sistemas la necesidad de contextualizar a la organización como sistema total, donde individuos, como tecnologías y los procesos involucrados en los servicios y las relaciones entre todos ellos, son parte de las mismas necesidades que deben gestionarse dentro del ámbito de las Tecnologías de la Información.

Adicionalmente el DSC-FI adopta al ISM3 como modelo de gestión de sus procesos por:

- Permitir la autoevaluación de la madurez de los procesos.
- Ser un modelo abierto (Permite la interacción con otros modelos o estándares.).
- Estar soportado internacionalmente y en continua mejora.
- Ser de acceso libre.
- Permitir el análisis con enfoque cualitativo.
- Permitir a la organización aprovechar la infraestructura actual, fortaleciéndola mediante un sistema de calidad, y alcanzado niveles de madurez certificables según el sistema evolucione.
- Ser útil para pequeñas y grandes organizaciones por lo niveles que son manejados.
- Dar la posibilidad de certificarse bajo ISO9001 o ISO27001.
- Contemplar la protección de inversión realizada en sistemas de manejo de la seguridad de la información y en prácticas y políticas propias de la organización.

Todo lo anterior retoma el trabajo realizado por el Departamento de Seguridad en Cómputo desde su creación en Septiembre de 2004, lo que permitirá una evolución organizacional en aspectos de la seguridad informática más acorde a los tiempos actuales, en donde tenemos regulaciones tanto internas, del ámbito nacional y hasta internacional, donde las necesidades actuales exigen mayor certidumbre en los procesos y servicios y más en temas de seguridad.

De manera resumida, ISM3 permitirá al Departamento de Seguridad en Cómputo cubrir la necesidad de un estándar simple y aplicable de calidad para los sistemas de gestión de la seguridad dentro de la Facultad de Ingeniería.

5.4 Evaluación de procesos dentro del Departamento de Seguridad en Cómputo

A continuación de manera práctica el ISM3 es utilizado para gestionar conforme a los criterios, metodología y documentación señalada en el capítulo cuatro de este trabajo de tesis, el proceso más importante para el Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSC-FI), la Atención a Incidentes de Seguridad en Cómputo.

Esto será el inicio para que de manera generalizada el DSC-FI ya con el fundamento técnico y operativo sobre el uso del ISM3 gestione de manera adecuada sus procesos.

EL ISM3 en este ejercicio será utilizado para evaluar la madurez que del proceso se tiene (atención a incidentes de seguridad en cómputo), Esta actividad se viene realizando desde la aparición del DSC-FI, y que con el paso del tiempo ha tenido cambios dado los nuevos vectores de ataque y las tecnologías y sofisticación utilizada por intrusos y usuarios malintencionados en su afán de provocar daños.

5.5 Adquisición del nivel de maduración por parte del Departamento de Seguridad en Cómputo

Se hizo una evaluación sobre el proceso que se tiene en el departamento y de esta manera determinar que el departamento se encontraba en el nivel 0 para posteriormente implementar los niveles de Gestión de Seguridad en el proceso y de esta manera llegar al nivel 1.

5.5.1 ISM3 Nivel 0

El DSC-FI se encontraba al inicio de este trabajo de tesis en el "Nivel ISM3 0", no se tenía implementado un Sistema de Gestión de Seguridad de la Información como tal, solo se tenía las bases que ayudaban a tener resultados favorables, sin embargo por el crecimiento de las amenazas, la interacción de otras áreas, el compromiso institucional de UNICA y del DSC-FI y el propósito de crear certidumbre en la atención de incidentes de seguridad en cómputo estaban siendo insuficientes las normas y metología que se tenían.

5.5.2 ISM3 Nivel 1

El alcance de este ejercicio permitirá ver si el proceso "Atención a Incidentes de Seguridad en Cómputo" tal como se lleva a cabo cumple y satisface los requerimientos del "Nivel ISM3 1", el cual permitirá observar de ser cierto, una disminución significativa del riesgo por amenazas técnicas con la inversión moderada que se tiene para ello.

5.5.2.1 Práctica genérica: Documentación

La siguiente documentación nos ayuda a verificar que el proceso de Atención a Incidentes de Seguridad en Cómputo este definido, robusto y repetible, permitiendo que el sistema ISM este actualizado.

Gestión de documentación

Práctica Genérica	**GP-1 Gestión de Documentación**
Descripción	El siguiente documento señala los mecanismos y actividades que el Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSC-FI), sigue para la atención de los incidentes de seguridad en cómputo que se presentan en y desde la Facultad de Ingeniería de la UNAM.
Fundamentación	Parte fundamental de la actividad del DSC-FI es la atención a Incidentes de Seguridad en Cómputo, la cual es además un actividad dentro del Plan del Desarrollo 2007-2011 de la FI, en su proyecto 5.7: "Seguridad y protección institucional" como parte del fortalecimiento de la seguridad informática de la institución.
Documentación	Políticas de Seguridad en Cómputo para la Facultad de Ingeniería. (www.ingenieri.unam.mx/~cacfi) Normatividad para la publicación de sitios Web. (www.ingenieri.unam.mx/~cacfi) Formato de reporte de atención a incidentes de seguridad en cómputo. Formato de inventario lógico de red.

Entradas	Descripción del proceso: Los incidentes de seguridad en cómputo pueden ser reportados por varias fuentes, las cuales son: la Dirección General de Servicios de Cómputo Académico, el mismo DSC-FI como parte de su actividad de monitoreo de la red, y a través de cualquier miembro de la comunidad en general. Responsabilidad: El DSC-FI es el responsable de recibir, analizar, priorizar y gestionar la atención del incidente en cuestión hasta su satisfactoria finalización.
Productos de Trabajo	**Reporte de Incidente de Seguridad en Cómputo:** La Facultad de Ingeniería es muy amplia por lo que su administración es compleja, esto lleva a tener diferentes Divisiones, Secretarías y Coordinaciones, a las que de manera personalizada se envía un oficio indicando el incidente que en su área se ha presentado. **Informes**: Una vez revisado o auditado el equipo involucrado en el incidente se envía un oficio, indicando la problemática detectada y las acciones y recomendaciones que deberán observarse para el aseguramiento del equipo. **Políticas**: los documentos que especifican requerimientos y reglas para el Proceso: • Las Políticas de Seguridad en Cómputo de la Facultad de Ingeniería. • La Normatividad para la publicación de sitios Web • Las políticas internas de cada área en caso de que existan. **Procedimientos**: El informe que mediante oficio se envía de la auditoría o revisión realizada reflejan de cómo el proceso se llevó a cabo, indicando adicionalmente la falta en que se incurrió, y las diferentes acciones que se deberán tomar en cuanto para evitar este tipo de problemas en un futuro. Estos documentos normalmente especifica: • Porque se realizó el procedimiento; • Quién lo aplicó; • Las responsabilidades de conformidad con el procedimiento; • Cuándo empieza y termina el procedimiento ; • Descripción paso a paso de las tareas (quién, qué, cuándo); • Cómo resolver y escalar los conflictos/excepciones;
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	Monitoreo del Esquema de Seguridad en Cómputo. Actualización del Inventario Lógico de Red.

	Mantenimiento y Actualización de las Políticas de Seguridad en Cómputo.
Metodologías relacionadas	NA

Tabla 5.1. GP-1 Gestión de Documentación

Tabla de Evaluación General

Los criterios de Documentado, Supervisado, y Aprovisionado se puntualizan de la siguiente manera:

Sí: 1
No: 0
Incompleto: 0.5
Se desconoce: -1

Posteriormente se calcula el puntaje promedio de un proceso el cuál se registra en la última columna de la tabla llamada Puntaje Global que es la suma de las 3 columnas de criterio. Para que un proceso obtenga un Aprobado, éste debe obtener 3 puntos.

En nuestro caso para el Proceso de Atención a Incidentes de Seguridad en Cómputo los resultados son los siguientes.

	Documentado	**Supervisado**	**Aprovisionado**	**Puntaje Global**
GP-1 Gestión de Documentación	1	1	1	3

Tabla 5.2. Evaluación de Documentación

La fundamentación de la evaluación realizada en esta tabla se trabaja en los subtemas siguientes.

El ISM3 puede certificarse asegurando que los procesos ISM cumplen con un estándar mínimo de calidad definido. La certificación está basada en evidencias y cada proceso se califica como *aprobado* si cumple con los siguientes criterios:

- **Documentado**: La documentación debe describir por completo el proceso e incluir plantillas y muestras de los productos del trabajo.
- **Supervisado**: Se requiere evidencia de que cada proceso tiene un Propietario del Proceso competente. Además, se requiere evidencia de que se reportan al Cliente la eficiencia y/o desempeño del proceso.
- **Aprovisionado**: Se requiere evidencia de que hay recursos adecuados en términos de presupuesto, personal y espacio para realizar el proceso. La Evidencia de que un proceso se lleva a cabo es suficiente para probar que está adecuadamente aprovisionado.

5.5.2.2 Práctica Específica: Gestión Estratégica

La Gestión Estratégica nos ayuda a tener informada a las autoridades sobre las acciones realizadas en el Departamento, además coordinar y asignar recursos para poder alcanzar la visión deseada del proceso.

Informe

Proceso	**SSP-1 Informar a las autoridades**
Descripción	Anualmente se genera un informe de la actividad relacionada a la atención de incidentes de seguridad en cómputo, reflejando los vectores que más fueron utilizados para atacar o comprometes los sistemas, esto es presentado de manera ejecutiva, y fundamenta las acciones para el año siguiente en cuando seguridad informática se refiere.
Fundamentación	Para tomar decisiones sobre las inversiones futuras y áreas de oportunidad del DSC-FI, las autoridades necesitan información sobre la atención de incidentes de seguridad en cómputo.
Documentación	Informe Anual de Atención de Incidentes de Seguridad en Cómputo.
Entradas	Informe del Detalle Técnico sobre atención de incidentes de seguridad en cómputo. Relación de reportes atendidos en el año.
Productos de Trabajo	Informe Anual de Atención de Incidentes de Seguridad en Cómputo.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	TSP-1 Informar a la gestión estratégica.
Metodologías relacionadas	NA

Tabla 5.3. SSP-1 Informar a las autoridades

Coordinación

Proceso	**SSP-2 Coordinar**
Descripción	Coordinación entre los Responsables de Cómputo de las diferentes áreas de la Facultad de Ingeniería (Divisiones, Secretarias y Coordinaciones) y el Responsable del DSC-FI.
Fundamentación	Se requiere coordinación entre el personal responsable de seguridad y los coordinadores de cómputo de las diferentes áreas de la organización para asegurar el soporte de toda la organización y ayudar a la organización a alcanzar sus objetivos y optimizar sus recursos.
Documentación	NA
Entradas	Seguridad de la Información y otros objetivos de Seguridad.

Productos de Trabajo	Procesos de Seguridad de la Información que soporta la organización.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.4. SSP-2 Coordinar

Visión Estratégica

Proceso	**SSP-3 Alcanzar visión estratégica**
Descripción	Identificación de los objetivos de la seguridad de la información en las siguientes áreas: • Ambiente y misión organizativa; • Cumplimiento de políticas y normatividades; • Protección de la privacidad; • Protección de la propiedad intelectual.
Fundamentación	El desarrollo de los Objetivos de Seguridad requiere un entendimiento estratégico del ambiente de la organización y de los objetivos de los diferentes servicios. Los objetivos de Seguridad proveen las bases para la Política de Seguridad de la Información y las Metas de Seguridad de la Información.
Documentación	NA
Entradas	Objetivos Organizativos. Atender al 100% todos los incidentes de seguridad en cómputo que se acontezcan dentro y desde la Facultad de Ingeniería de la UNAM.
Productos de Trabajo	Política de Seguridad de Seguridad en Cómputo. Este es el documento clave para la gestión estratégica de la seguridad de la información. Incluye: • Objetivos de Seguridad de la Información; • Requerimientos de Seguridad de la Información para el Personal, académicos, alumnos y suministradores.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	TSP-3 Definir las de Metas de Seguridad. TSP-12 Seleccionar los procesos específicos.
Metodologías relacionadas	NA

Tabla 5.5. SSP-3 Alcanzar visión estratégica

Asignación de Recursos

Proceso	**SSP-6 Asignar recursos para la seguridad de la información**
Descripción	Este Proceso Asigna los recursos como personal, presupuesto e infraestructura para la gestión táctica y operativa.
Fundamentación	La implementación de un sistema ISM requiere inversión en Procesos de gestión táctica y operativa.
Documentación	Presupuesto para la Seguridad de la Información.
Entradas	Requerimiento de Presupuesto para la Seguridad de la Información.
Productos de Trabajo	Presupuesto de Seguridad de la Información. Recursos destinados a la Gestión de Seguridad de la Información.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo. Coordinador de la Unidad de Servicios de Cómputo Académico. Secretario General. Secretario Administrativo.
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.6. SSP-6 Asignar recursos para la seguridad de la información

Tabla de Evaluación de Gestión Estratégica

	Documentado	**Supervisado**	**Aprovisionado**	**Puntaje Global**
SSP-1 Informar a las autoridades	1	1	1	3
SSP-2 Coordinar	1	1	1	3
SSP-3 Alcanzar visión estratégica	1	1	1	3
SSP-6 Asignar recursos para seguridad de la información	1	1	1	3

Tabla 5.7. Evaluación de Gestión Estratégica

5.5.2.3 Práctica Específica: Gestión Táctica

La Gestión Táctica es la responsable del desempeño del ISM, para esto se definen las Metas de Seguridad y posteriormente realizar lo necesario para alcanzarlas utilizando los recursos del departamento de la mejor manera.

Informe

Proceso	**TSP-1 Informar a la gestión estratégica**
Descripción	Informar regularmente sobre los resultados de atención de incidentes y de uso de los recursos Asignados.
Fundamentación	Se requiere un informe al cuerpo directivo para demostrar el desempeño, eficiencia y efectividad del proceso de atención de incidentes de seguridad en cómputo.
Documentación	Informe Anual de Atención de Incidentes de Seguridad en Cómputo.
Entradas	Informe anual sobre incidentes de seguridad en cómputo de la Dirección General de Servicios de Cómputo académico. Informe del Detalle Técnico sobre atención de incidentes de seguridad en cómputo. Relación de reportes atendidos en el año.
Productos de Trabajo	Informe Anual de Atención de Incidentes de Seguridad en Cómputo.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	OSP-1 Informar a la gestión táctica.
Metodologías relacionadas	NA

Tabla 5.8. TSP-1 Informar a la gestión estratégica.

Gestión de recursos

Proceso	**TSP-2 Gestionar los recursos asignados**
Descripción	La Secretaría General a través de la Coordinación de la Unidad de Servicios de Cómputo Académico asigna los recursos para todos los Procesos Tácticos y Operativos.
Fundamentación	Se requiere planificación y control de la Asignación de los recursos para asegurar que la atención a incidentes de seguridad en cómputo esté configurada para alcanzar las Metas de Seguridad.
Documentación	Presupuesto para la Seguridad de la Información.
Entradas	Planes de Proceso. Presupuesto de Seguridad de la Información.
Productos de Trabajo	Recursos asignados al Proceso.

Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	SSP-6 Asignar recursos para la seguridad de la información.
Metodologías relacionadas	NA

Tabla 5.9. TSP-2 Gestionar los recursos asignados.

Metas de seguridad

Proceso	**TSP-3 Definir las Metas de Seguridad**
Descripción	Este proceso transforma los Objetivos de Seguridad en Metas de Seguridad medibles, realizables con los recursos disponibles y relacionadas con bienes o clases de bienes específicos.
Fundamentación	La alineación de las Metas de Seguridad con los Objetivos de Seguridad de la organización provee las bases del proceso para alcanzar un nivel de seguridad apropiado.
Documentación	NA
Entradas	Política de Seguridad en Cómputo
Productos de Trabajo	Meta en la Atención de Incidentes de Seguridad en Cómputo - Contar con redes y sistemas sanos. - Fortalecer la cultura de seguridad informática - Tratar los problemas de seguridad en cómputo antes de que trasciendan de manera crítica.
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	SSP-3 Alcanzar visión estratégica.
Metodologías relacionadas	NA

Tabla 5.10. TSP-3 Definir las Metas de Seguridad.

Selección segura de procesos

Proceso	**TSP-12 Seleccionar procesos específicos**
Descripción	Este Proceso selecciona los Procesos operativos más apropiados para alcanzar las Metas de Seguridad.
Fundamentación	Toda organización tiene diferentes Metas de Seguridad, se desenvuelve en diferentes ambientes y posee diferentes recursos. Una selección apropiada de Procesos alcanzará un buen retorno de la inversión en seguridad.
Documentación	NA

Entradas	Metas de Seguridad de la Información. Presupuesto de Seguridad de la Información. Inventario de Bienes. Informes de Incidentes. Informes de Intrusiones. Informes Forenses.
Productos de Trabajo	Definición de Procesos de Gestión de Seguridad de la Información. Informe de Amenazas a Asegurar. Políticas de Procesos de Seguridad: • Política de Control de Segmentación y Filtrado; • Política de Gestión de Resguardo y Redundancia; • Política de Control de Acceso; • Política de Concesión de Solicitudes de Acceso; • Política de Protección contra Malware; • Política de Investigación de Incidentes; • Política de Gestión de Cifrado;
Propietario del Proceso	El Responsable del Departamento de Seguridad en Cómputo.
Procesos relacionados	TSP-3 Definir las Metas de Seguridad. SSP-6 Asignar recursos para la seguridad de la información.
Metodologías relacionadas	Evaluación de Amenazas: NA Análisis de Riesgos: OCTAVE

Tabla 5.11. TSP-12 Seleccionar procesos específicos

Tabla de Evaluación de Gestión Táctica

	Documentado	**Supervisado**	**Aprovisionado**	**Puntaje Global**
TSP-1 Informar a la gestión estratégica.	1	1	1	3
TSP-2 Gestionar los recursos asignados.	1	1	1	3
TSP-3 Definir las Metas de Seguridad.	1	1	1	3
TSP-12 Seleccionar procesos específicos.	1	1	1	3

Tabla 5.12. Evaluación de Gestión Táctica

5.5.2.4 Práctica Específica: Gestión Operativa

La Gestión Operativa proporciona medidas para proteger los bienes y sistemas de información del departamento. Gestionando el proceso para la prevención y detección de incidentes.

Informe

Proceso	OSP-1 Informar a la gestión táctica
Descripción	Un informe regular de los resultados del Proceso y el uso de los recursos Asignados.
Fundamentación	Para mostrar el desempeño y la efectividad del Proceso en uso, se requiere informar a la Coordinación de la Unidad de Servicios de Cómputo Académico.
Documentación	Informe Operativo de Seguridad en Cómputo.
Entradas	Datos de indicadores Operativas
Productos de Trabajo	Informe Operativo de Seguridad de la Información. Como la Gestión Operativa lidia principalmente con la prevención y mitigación de incidentes.
Propietario del Proceso	Departamento de Seguridad en Cómputo
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.13. OSP-1 Informar a la gestión táctica.

Parcheo del ambiente

Proceso	OSP-5 Refaccionar el ambiente
Descripción	Este Proceso cubre la actualización de servicios para prevenir los incidentes relacionados con debilidades conocidas.
Fundamentación	Las actualizaciones previenen que ocurran incidentes de la explotación de debilidades conocidas en los servicios.
Documentación	Boletines de Actualización de los Servicios. Política de Seguridad en Cómputo.
Entradas	Informe de Alertas y Correcciones.
Productos de Trabajo	Servicios actualizados en todos los ambiente.
Propietario del Proceso	Departamento de Seguridad en Cómputo
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.14. OSP-1 Informar a la gestión táctica**.**

Gestión de Resguardo y Redundancia

Proceso	**OSP-10 Gestionar el respaldo y redundancia**
Descripción	Este es un conjunto de medidas de seguridad para reducir el impacto de fallos o pérdidas de equipamiento.
Fundamentación	Los incidentes ocasionados por la pérdida de respaldos y discontinuidad de canales, interfaces y servicios pueden ser mitigados mediante Procesos de resguardo y la eliminación de los puntos únicos de falla.
Documentación	Procedimiento de respaldos. Procedimiento de Redundancia. Definición de Prioridades.
Entradas	Inventario lógico de red. Informe de Detección de Incidentes.
Productos de Trabajo	Prevención contra pérdida de información permanente en los respaldos. Prevención contra interrupción de canales, interfaces y servicios. Informe de Resguardo. Informe de Recuperación. Informe de Estado de Redundancia.
Propietario del Proceso	Departamento de Seguridad en Cómputo
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.15. OSP-10 Gestionar el respaldo y redundancia

Gestión del Filtrado y Segmentación

Proceso	**OSP-16 Gestionar el filtrado y segmentación**
Descripción	Este Proceso define las políticas técnicas para el paso de mensajes autorizados entre zonas, mientras se deniega el paso de mensajes no autorizados.
Fundamentación	Los incidentes causados por la intrusión, vandalismo y abuso de los sistemas de información pueden ser prevenidos y mitigados mediante la segmentación apropiada de los ambientes y respaldos y con el filtrado de mensajes.
Documentación	Política de Seguridad en Cómputo.
Entradas	Informa del Esquema de Seguridad Perimetral en Cómputo. Informe de Detección de Incidentes. Informe de Detección de Intrusiones.
Productos de Trabajo	Prevención contra el pasaje no autorizado de mensajes entre ambientes. Registro del uso de canales.

Propietario del Proceso	Departamento de Seguridad en Cómputo.
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.16. OSP-16 Gestionar el filtrado y segmentación

Protección contra Malware

Proceso	**OSP-17 Gestionar la protección contra malware**
Descripción	Este es un conjunto de medidas de seguridad para proporcionar protección contra amenazas técnicas como virus, spyware, troyanos, puertas traseras, key loggers y otros servicios no autorizados.
Fundamentación	Los incidentes relacionados con la infección de bienes con Malware pueden ser prevenidos y mitigados por un apropiado Proceso de protección contra Malware.
Documentación	Procedimiento de Protección contra Malware.
Entradas	Proyecto Malware de la Facultad de Ingeniería. Informe de Detección de Incidentes.
Productos de Trabajo	Protección de los sistemas de información contra el Malware. Informe de Limpieza y Detección de Malware. Informe del Nivel de Actualización y despliegue de Protección contra Malware.
Propietario del Proceso	Departamento de Seguridad en Cómputo.
Procesos relacionados	NA
Metodologías relacionadas	NA

Tabla 5.17. OSP-17 Gestionar la protección contra malware

Tabla de Evaluación de Gestión operativa

	Documentado	**Supervisado**	**Aprovisionado**	**Puntaje Global**
OSP-1 Informar a la gestión táctica.	1	1	1	3
OSP-5 Refaccionar el ambiente.	1	1	1	3
OSP-10 Gestionar el respaldo y redundancia.	1	1	1	3

OSP-16 Gestionar el filtrado y segmentación.	1	1	1	3
OSP-17 Gestionar la protección contra Malware	1	1	1	3

Tabla 5.18. Evaluación de Gestión operativa

5.5.3 Resultados adquiridos

En el inicio de la verificación de la madurez del proceso de atención a incidentes de seguridad en cómputo por parte del DSC-FI no se tenía toda la información y documentación que el proceso requería para cumplir con el Nivel "ISM3 1".

Sin embargo este ejercicio ha permitido iniciar una gestión sólida del proceso y hoy en día el Departamento de Seguridad en Cómputo de la Facultad de Ingeniería puede afirmar que cumple con el "Nivel ISM3 1" ya que ha cubierto todos los elementos necesarios y está en proceso de alcanzar el "Nivel ISM3 2".

Conclusiones

Se ha cumplido satisfactoriamente el objetivo de este trabajo de tesis, definiendo de manera sistemática y documentada, el modelo de gestión que el Departamento de Seguridad en Cómputo de la Facultad de Ingeniería (DSC-FI), de la UNAM debía adoptar en sus procesos.

El resultado obtenido evita depender de métodos caros de análisis de riesgos y de gestión de procesos, que suponen una barrera a la implantación de sistemas de Gestión de Seguridad de la Información (ISM, por sus siglas en Inglés) en la organización; he podido fijar las bases para la implementación sólida y con perspectivas a corto plazo del "Modelo de Madurez en la Administración de la Seguridad Informática (ISM3)", en los procesos del Departamento de Seguridad en Cómputo.

De esta manera el DSC-FI podrá garantizar que los riesgos en la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y las tecnologías dentro de la institución.

Este trabajo de tesis a su vez presenta un enfoque general sobre el tratamiento de la seguridad informática, sin particularizar en los elementos propios de las Tecnologías de la Información, sino que reconoce y acepta como parte del proceso de aseguramiento de redes y sistemas la necesidad de contextualizar a la organización como sistema total, donde individuos, como tecnologías y los procesos involucrados en los servicios y las relaciones entre todos ellos, son parte de las mismas necesidades que deben gestionarse dentro del ámbito de las Tecnologías de la Información; situación que muy pocas veces es considerada.

De esta manera, el presente documento además de cubrir una gran necesidad del DSC-FI, representa una muy adecuada referencia para toda aquella organización que desea hacer efectivo todo el potencial que sus Tecnologías de la Información le ofrecen, observando a estas como parte del todo y no un complemento o herramienta aislada.

Entre las consideraciones fundamentales por las que el "Modelo de Madurez en la Administración de la Seguridad Informática (ISM3)" fue adoptado se tienen:

- Que permite la autoevaluación de la madurez de los procesos.
- Es modelo abierto (Permite la interacción con otros modelos o estándares).
- Esta soportado internacionalmente y en mejora continua.
- Es de acceso libre.
- Permite el análisis con enfoque cualitativo.
- Permite a la organización aprovechar la infraestructura actual, fortaleciéndola mediante un sistema de calidad, y alcanzado niveles de madurez certificables según el sistema evolucione.

- Es útil para pequeñas y grandes organizaciones por lo niveles de madurez que son manejados.

- Da la posibilidad de certificarse bajo ISO9001 o ISO27001.

- Contempla la protección de inversión realizada en sistemas de manejo de la seguridad de la información, en prácticas y políticas propias de la organización.

Es importante destacar, que gracias a este trabajo fue posible que el proceso más importante del Departamento de Seguridad en Cómputo de la Facultad de Ingeniería: "Atención a Incidentes de Seguridad en Cómputo", pasara de un NIVEL ISM3 0 a un NIVEL ISM3 1, mediante el ordenamiento, organización, trabajo en equipo y en algunos casos la generación de documentación para fundamentar la madurez del proceso, lo que refleja el empeño y compromiso del DSC-FI de mejorar la calidad de sus servicios.

Este cambio de nivel ha permitido al DSC-FI iniciar una gestión sólida del mismo proceso y es la punta de lanza para replicar la actividad en los demás procesos del Departamento. El Nivel ISM3 1 ha permitido observar una disminución significativa en la cantidad de incidentes ya que con la metodología aplicada atiende el problema e identifica las situaciones que lo suscitaron y estos también son considerados para evitar la repetición del problema.

Finalmente puedo decir que el "Modelo de Madurez en la Administración de la Seguridad Informática (ISM3)" permitirá al Departamento de Seguridad en Cómputo cubrir la necesidad de un estándar simple y aplicable de calidad para los sistemas de gestión de la seguridad dentro de la Facultad de Ingeniería.

Recomendaciones

Uno de los componentes primordiales en la implantación exitosa de ISM3 en el Departamento de Seguridad en Cómputo es la participación de las autoridades. Se debe asumir desde un principio que un Sistema de Gestión de la Seguridad Informática afecta fundamentalmente a la gestión de la Facultad y requiere, por tanto, de decisiones y acciones que sólo las autoridades pueden tomar. Es importante no caer en el error de considerar que el Modelo de Madurez de Gestión de la Seguridad de la Información (ISM3) es una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; puesto que se están gestionando riesgos e impactos de servicios que son responsabilidad y decisión de las autoridades. Los cuáles deben comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del sistema de gestión. Por lo que se le asigna la tarea de al menos una vez al año, revisar el sistema de gestión, para asegurar que continúe siendo adecuado y eficaz.

También es importante la formación y la concienciación en seguridad de la información ya que son elementos básicos para el éxito del ISM3. Por ello, se debe asegurar que todo el personal de la Facultad a la que se le asignen responsabilidades definidas en el sistema de gestión esté suficientemente capacitado. Además, las autoridades deben asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del ISM3.

Al finalizar esta tesis se dejó funcionando al proceso más importante del DSC-FI "Atención a Incidentes de Seguridad en Cómputo" en el NIVEL ISM3 1 pero con las bases para llevarlo a los demás niveles de maduración. Ya con los fundamentos se podrá trabajar con otros procesos creados en el departamento.

Con la madurez de los procesos y la participación de las autoridades y personal involucrado tenemos la posibilidad de ir obteniendo una madurez en el Sistema de Gestión de Seguridad de la Información llevando al DSC-FI a otra etapa donde se pueda ser auditado por alguna organización especializada como el UNAM-CERT.

Al ser auditados esperamos haber llegado a una madurez en el sistema ISM3 y buscar un modelo certificable como ISO 9001 o ISO 270001 los cuales son costosos si se realizan sin ninguna base pero ya teniendo el ISM3 en su madurez final el costo de la certificación se reducirá enormemente, teniendo la garantía que nuestros sistemas son gestionados y protegidos debidamente.

ANEXO A

TABLAS DE NIVELES DE GESTIÓN DE SEGURIDAD

Los siguientes anexos nos muestran los procesos que deben ser implementados en los niveles de madurez, se requiere que cada uno tenga su descripción completa para poder ser evaluado.

A continuación se muestra la tabla que debe ser llenada por los procesos, del lado derecho se encuentran los nombres de las propiedades fundamentales del proceso y del lado izquierdo la descripción de cada uno.

Proceso	**Código y denominación del proceso**
Descripción	La actividad realizada por el proceso.
Fundamentación	Cómo contribuye el proceso a los objetivos específicos y globales.
Documentación	Políticas, Procedimientos y Plantillas de Definiciones de Procesos que necesitan ser descritas o realizadas por el proceso.
Entradas	Entradas al proceso. Las entradas en *cursiva* pueden obtenerse de fuentes que no tienen por qué ser documentos.
Productos de Trabajo	Resultados del proceso. Los productos de trabajo en *cursiva* son productos distintos de documentos.
Propietario del Proceso	Un ejemplo de Propietario del Proceso se da en esta fila. Cada proceso debería tener un y sólo un Propietario del Proceso. Cuando un grupo de personas, como gestores de servicios, son referidos como un Propietario del Proceso, esto significa que cada uno de ellos es responsable de una instancia separada del proceso.
Procesos relacionados	Otros procesos ISM3 que son necesarios para generar las entradas clave.
Metodologías relacionadas	Metodologías y mejores prácticas bien conocidas. Estas metodologías pueden ser útiles para identificar actividades relevantes, riesgos y controles.

Tabla Descripción de los procesos a alto nivel

PRÁCTICA GENÉRICA: DOCUMENTACIÓN

Las siguientes tablas nos ayudan al proceso de documentación cuya finalidad es tener un proceso definido, robusto y repetible.

Tabla de Evaluación General

	Documentado	Supervisado	Aprovisionado	Puntaje Global
GP-1 Gestión de Documentación.				

PRÁCTICA ESPECÍFICA: GESTIÓN ESTRATÉGICA

Las siguientes tablas nos ayudan a tratar los objetivos globales y la provisión de recursos para cubrir la gestión estratégica.

Tabla de Evaluación de Gestión Estratégica

	Documentado	Supervisado	Aprovisionado	Puntaje Global
SSP-1 Informar a las autoridades.				
SSP-2 Coordinar.				
SSP-3 Alcanzar visión estratégica.				
SSP-4 Definir las reglas para la separación de responsabilidades: transparencia, particionado, supervisión, rotación y separación de responsabilidades (TPSRSR).				
SSP-5 Comprobar el cumplimiento con las reglas TPSRSR.				
SSP-6 Asignar recursos para seguridad de la información.				

PRÁCTICA ESPECÍFICA: GESTIÓN TÁCTICA

La Gestión Táctica nos ayuda en los objetivos específicos y la gestión de los recursos de la organización, para esto es necesario cubrir con los documentos descritos en cada una de las siguientes tablas.

Tabla de Evaluación de Gestión Táctica

	Documentado	Supervisado	Aprovisionado	Puntaje Global
TSP-1 Informar a la gestión estratégica.				
TSP-2 Gestionar los recursos asignados.				
TSP-3 Definir las Metas de Seguridad.				
TSP-4 Definir los indicadores para los procesos de seguridad.				
TSP-5 Definir grupos de propiedades.				
TSP-6 Definir ambientes y ciclos de vida.				
TSP-7 Investigar antecedentes y referencias.				
TSP-8 Seleccionar el personal de seguridad.				
TSP-9 Capacitar al personal de seguridad.				
TSP-10 Definir procesos disciplinarios.				
TSP-11 Alcanzar conciencia en seguridad.				
TSP-12 Seleccionar procesos específicos.				

PRÁCTICA ESPECÍFICA: GESTIÓN OPERATIVA

Con las siguientes tablas encontramos los documentos que deben ser llenados para llevar a cabo la parte operativa y de esta manera informamos a las autoridades y al equipo de gestión táctico sobre la seguridad de la información y el logro de los objetivos definidos.

Tabla de Evaluación de Gestión operativa

	Documentado	Supervisado	Aprovisionado	Puntaje Global
OSP-1 Informar a la gestión táctica.				
OSP-2 Seleccionar las herramientas para implementar las medidas de seguridad.				
OSP-3 Gestionar el inventario.				
OSP-4 Controlar el cambio del ambiente de los sistemas de información.				
OSP-5 Refaccionar el ambiente.				
OSP-6 Limpiar el ambiente.				
OSP-7 Fortalecer el ambiente.				
OSP-8 Controlar el ciclo de vida del desarrollo de software.				
OSP-9 Controlar los cambios en las medidas de seguridad.				
OSP-10 Gestionar el respaldo y redundancia.				
OSP-11 Controlar el acceso a servicios, canales, repositorios e interfaces.				
OSP-12 Llevar el registro de usuarios.				

OSP-13 Gestionar el cifrado.				
OSP-14 Gestionar la protección del ambiente físico.				
OSP-15 Gestionar la continuidad de operaciones.				
OSP-16 Gestionar el filtrado y segmentación.				
OSP-17 Gestionar la protección contra Malware				
OSP-18 Gestionar el aseguramiento.				
OSP-19 Emular ataques, errores y accidentes.				
OSP-20 Emular incidentes.				
OSP-21 Comprobar la calidad de la información				
OSP-22 Monitorizar alertas.				
OSP-23 Detectar y analizar los eventos.				
OSP-24 Manejar los incidentes y pseudoincidentes				
OSP-25 Realizar el análisis forense.				

Glosario

A

Acceso: Con respecto a la privacidad, es la habilidad de un individuo para ver, modificar y refutar lo completa y precisa que pueda ser la información reunida sobre él o ella.

Accidente: Un incidente con una causa natural no humana.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Cualquier cosa que tiene valor para la organización.

Alarma: Un conjunto de eventos causados probablemente por un incidente.

Alerta: Una advertencia de una posible vulnerabilidad.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Ambiente (Entorno):
1. Todos los factores externos, físicos, lógicos y Organizativos de una organización.
2. Una zona técnica de la organización con un propósito definido, como un ambiente de Servidor, un ambiente de Cliente, un ambiente de Desarrollo, etc.
3. Cualquier subdivisión de una división Organizativa, técnica o lógica bajo un solo equipo de gestión.

Amenaza: Una causa potencial de un Ataque, Incidente o Error.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Antivirus: Es el software diseñado específicamente para la detección y prevención de virus conocidos.

Ataque: Un incidente con una causa intencional humana.

Ataque por servicio denegado - DoS (s) - Denial of Service attack: Es un asalto computarizado llevado a cabo por un atacante para sobrecargar o congelar un servicio de red, como un servidor Web o de archivos. Por ejemplo, un ataque puede causar que el servidor esté tan ocupado tratando de responder, que ignorará cualquier petición legítima de conexión.

Auditor: Alguien externo a la organización que comprueba en nombre del Propietario del Proceso o el Cliente.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Es el proceso de verificar que alguien o algo es quien o lo que dice ser. En redes de equipos públicos y privados (incluyendo Internet), la autenticación se lleva a cabo comúnmente a través de contraseñas de inicio de sesión.

Autoridad: La persona técnica que implementa los Solicitudes de Acceso aprobadas.

Autorización: Con referencia a la computación, especialmente en los equipos remotos en una red, es el derecho otorgado a un individuo o proceso para utilizar el sistema y la información almacenada en éste. Típicamente la autorización es definida por un administrador de sistemas y verificado por el equipo basado en alguna identificación del usuario, como son un código o una contraseña.

Autorizador: Un delegado de un Propietario del Sistema de Información que puede aprobar o denegar las Solicitudes de Acceso a interfaces, repositorios, canales y servicios de un sistema de información.

B

Bien: Cualquier propiedad valiosa de una organización.

BS7799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información -no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de estos últimos.

BSI: British Standards Institution. Comparable al AENOR español, es la Organización que ha publicado la serie de normas BS 7799, además de otros varios miles de normas de muy diferentes ámbitos.

C

Caballo de Troya (troyano): Es un programa computacional que aparentemente es útil pero que en realidad causa daño.

Calidad: El alcanzar o sobrepasar las expectativas.

Calidad en el servicio – QoS: Es un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de información.

Canal: Un canal es un medio usado por los servicios para intercambiar mensajes en forma transparente, sin ayuda explícita de otros servicios de niveles más bajos. Esta colaboración es normalmente necesaria para crear y cerrar canales lógicos.

Catástrofe: Cualquier incidente que puede resultar en la desaparición de la organización.

Certificado: Es un archivo encriptado que contiene información de identificación del usuario o servidor, la cual es utilizada para verificar la identidad y ayudar a establecer un vínculo de seguridad mejorada.

Checklist : Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Ciclo de vida: El conjunto de estados que conforman la serie de condiciones operativas de un sistema de información.

Clasificación: Una medida cualitativa del nivel de secreto de un bien de información.

Cliente: El cliente de un Proceso provee los recursos y el conjunto de requerimientos del Proceso.

CobiT: Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

COSO: Committee of Sponsoring Organizations of the Treadway Commission. Comité de Organizaciones Patrocinadoras de la Comisión Treadway. Se centra en el control interno, especialmente el financiero.

Crítico: Crítico es la medida más alta de prioridad de un servicio. Un servicio es crítico en un intervalo de tiempo si la interrupción del mismo por un período de tiempo mayor pondría en riesgo a la organización con una alta probabilidad. Por consiguiente, los servicios pueden ser priorizados en función de los segundos, minutos y horas que la organización pueda sobrevivir sin que esté disponibles.

D

Debilidad: Cualquier defecto en los servicios, mensajes, canales, repositorios, interfaces, Procesos Organizativos o asignación de responsabilidades que proporcionen una oportunidad para un error, ataque o accidente.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas

Disponibilidad: El porcentaje del Tiempo total de un servicio, interfase, o canal que debe funcionar continuamente.

Durabilidad: Una medida cualitativa de la cantidad de tiempo durante la cual un tipo de información debe ser obtenible.

E

Encriptación: Se refiere al proceso de convertir datos en texto cifrado para evitar que terceras personas lo puedan ver o acceder.

Entidad de acreditación: Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina)...

Entidad de certificación: Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27000, ISO 9000, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Error: Un incidente causado por alguien debido a una incongruencia entre el resultado efectivo de una tarea y el pretendido, o bien por falta de la información necesaria, o ésta era incorrecta.

Evaluación de riesgos: Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Cualquier hecho que pueda llevar a la detección de un incidente.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Expectativa: Cualquier esperanza de un estado futuro de bienes, Procesos Organizativos o sistemas de información.

F

Fiabilidad: El porcentaje de tiempo Disponible de un servicio, interfase o canal en el cual debe estar funcionando plenamente.

G

Gestión: Gestionar algo es:

- Definir y alcanzar Objetivos.
- Optimizar el uso de Recursos.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

H

HIPAA: Véase Ley de Explicación y Portabilidad del Seguro de Salud.

I

IEC: International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Impacto: El costo directo e indirecto de un incidente incluyendo el costo de restaurar los bienes a un estado anterior al incidente.

Incidente: Una falla en alcanzar un objetivo de seguridad resultado de un accidente, error o ataque.

Información confidencial: Desde la perspectiva de la Unión Europea, es la, información personal identificable que se refiera a raza u origen étnico, opiniones políticas, creencias religiosas o filosóficas, preferencias sexuales o membresía a sindicatos de comercio. Dentro de los Estados Unidos, la información confidencial también incluye información sobre salud, finanzas e hijos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Interfaz: Un medio de entrada / salida o entre un usuario y un sistema de información.

Intrusión: El robo de información sobre un objetivo por un atacante.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: Information Systems Audit and Control Association. Publica CobiT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISMS: Information Systems Management System. Véase: SGSI.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ITIL: IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

ITSEC: Criterios de evaluación de la seguridad de la tecnología de información. Se trata de criterios unificados adoptados por Francia, Alemania, Holanda y el Reino Unido. También cuentan con el respaldo de la Comisión Europea (véase también TCSEC, el equivalente de EEUU).

L

Ley de Explicación y Portabilidad del Seguro de Salud – HIPAA: Reglamento de los EE.UU. que otorga a los pacientes mayor acceso a sus propios archivos médicos y más control sobre cómo se utiliza su información personal identificable de salud. La regulación también habla de las obligaciones que tienen los proveedores y planes de salud de proteger la información. En general, las entidades cubiertas como son planes de salud, cámaras de compensación, y proveedores de salud quienes conducen ciertas transacciones financieras y administrativas electrónicamente tienen hasta el 14 de Abril del 2003 para cumplimentar esta ley.

Ley de Modernización Financiera de 1999: Financial Modernization Act of 1999 Véase Ley Graham-Leach-Billey.

Ley Graham-Leach-Billey – GLB: Ley de los Estados Unidos que contiene disposiciones que requieren que todas las instituciones financieras expongan a los consumidores y clientes, sus políticas y prácticas para proteger la privacidad de información personal no pública. La información personal no pública incluye cualquier información personal identificable proporcionada por un cliente, que resulte de una transacción con la institución financiera u obtenida por la institución financiara a través del suministro de productos o servicios. También conocida como la Ley de Modernización Financiera de 1999.

Límite: La frontera entre dos ambientes o sistemas de información que tienen características distintas.

M

Mensaje: Datos con significado intercambiados entre servicios en un manera jerárquica o entre iguales.

Meta de Seguridad: Un requerimiento derivado de un objetivo de seguridad, especificado cuantitativamente y relacionado a un bien o clase de bien de información.

Mejor práctica: Una regla de seguridad especifica a una plataforma que es aceptada en la organización al proporcionar un enfoque más efectivo a la implementación de seguridad concreta.

N

Nodo: Un sistema de información cuya función primaria es enrutar mensajes entre canales.

O

Objetivo: Un bien de información el cual puede ser víctima o víctima potencial de un ataque.

Objetivo de Seguridad: Una expectativa o requerimiento de negocio que depende de un Proceso de seguridad.

Objetivo Específico: Un objetivo de un conjunto de prácticas específicas.

Objetivo Genérico: Un objetivo que se alcanza cuando se logra un conjunto de Objetivos Específicos.

Oportunidad: La combinación de un bien, una amenaza y una ocasión que pueda dar origen a un incidente.

P

Partición: Cualquier subdivisión de un todo que no se yuxtapone total o parcialmente con cualquier otra subdivisión.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Política: Declaración general de principios que representa la posición de la administración para un área de control definida, con el fin de aplicarlas a largo plazo para guiar el desarrollo de nuevas reglas y criterios más especificas que aborden situaciones concretas.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Intención y dirección general expresada formalmente por la Dirección.

Práctica Específica: Un proceso.

Práctica Genérica: Un Proceso auxiliar de una práctica específica para alcanzar un objetivo genérico.

Prioridad: Una medida cualitativa del potencial de una falla o pérdida de causar problemas en el desempeño de una red o un servicio en la continuidad y misión de una organización.

Privacidad: El control que los clientes tienen sobre la recolección, uso y distribución de su información personal.

Privilegios: Es el permiso otorgado a un usuario para llevar a cabo una tarea específica, usualmente una que afecta a todo un sistema computacional en lugar de a un objeto en particular. Los privilegios son asignados por un administrador, a usuarios individuales o a grupos de usuarios, como parte de las configuraciones de seguridad de una PC.

Probador: Alguien en la organización comprobando en representación del Propietario del Proceso.

Procedimiento: Definen específicamente las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada; son dependientes de la tecnología y de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos.

Proceso: Un conjunto de tareas que producen productos y servicios.

Procesos Estratégicos: Procesos que determinan los objetivos de los Procesos de niveles más bajos.

Proceso Operativo: Un Proceso que cumple con los requerimientos de la Gestión Táctica.

Procesos Tácticos: Procesos que proveen un marco para los procesos operacionales. Estos Procesos normalmente lidian con la gestión de recursos (gente, dinero, tiempo, información, infraestructura, etc.).

Propietario del Proceso: La persona o equipo responsable del Proceso.

Propietario del Sistema de Información: El Cliente [ITIL] de un sistema de información, el cual posee todos los derechos del sistema, incluyendo su eliminación.

R

Rechazo: La habilidad de un usuario para negar haber llevado a cabo una acción que otras partes no puedan refutar. Por ejemplo, un usuario que borre un archivo puede con éxito negar haberlo hecho si no existe ningún mecanismo (como archivos de auditoria) que pueda contradecir su declaración.

Recurso: Un recurso es cualquier cosa necesaria para completar una tarea. Muchos recursos dejan de estar disponibles para otras tareas cuando comienzan a utilizarse. Algunos recursos se agotan al usarse y no puede ser reutilizados.
Algunos recursos fundamentales son Tiempo, Dinero, Personas, Logística e Infraestructura e Información.

Red: Un conjunto de canales físicos o lógicos que conectan repositorios e interfaces.

Repositorio: Cualquier almacenamiento permanente o transitorio de información.

Responsabilidad: Una asignación de una tarea, con poder y recursos, a un individuo competente o a un equipo responsable de la ejecución apropiada de la tarea.

Riesgo: Las pérdidas esperadas en función de la probabilidad e impacto de un conjunto de incidentes, medidas en unidades monetarias anuales. El riesgo máximo es la certeza de perder el valor total de la organización en un año o menos.

Rol: Un conjunto de responsabilidades.

S

Sarbanes-Oxley: Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para

supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

Secreto: Información compartida en una forma controlada entre un grupo de personas.

Seguridad: El logro reiterado de Objetivos de Seguridad.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Servicio: Un código o programa que provee de valor a usuarios, mediante el intercambio de mensajes con otros servicios y el acceso a Repositorios.

SGSI (Sistema de Gestión de la Seguridad de la Información): (Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información. La parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Sistema de Información: Una infraestructura técnica o humana para almacenar, procesar, transmitir, y dar entrada y salida a información.

Suplantación: Es la habilidad de un proceso para ejecutarse en un contexto de seguridad específica - como un usuario específico, por ejemplo - y por tanto acceder recursos autorizados para ese contexto de seguridad. La suplantación es utilizada en las aplicaciones Web para proporcionar un contexto de seguridad mejorada para peticiones anónimas.

T

TCSEC: Criterios de evaluación de la seguridad de los sistemas de computación, conocidos también con el nombre de Orange Book (Libro naranja), definidos originalmente por el Ministerio de Defensa de los EE.UU. Véase también ITSEC, el equivalente europeo.

TPSRSR: Acrónimo de Transparencia, Particionado, Supervisión, Rotación y Separación de Responsabilidades.

U

Usuario: La persona que usa un sistema de información.

V

Valoración de riesgos: Proceso completo de análisis y evaluación de riesgos.

Virus: Programa que trata de esparcirse de una PC a otra, usualmente a través de correo electrónico, adjuntándose a si mismo a un programa huésped. Puede dañar el hardware, software o datos. Compare con gusano.

Visibilidad: El grado en que los bienes de información en los bordes presentan una interfase o proveen servicios a sistemas de información externos a la organización.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo. Exposición latente a un riesgo

Bibliografía

Capítulo 1

1. **NUÑEZ** Sandoval Alejandro, *"Administración y planeación de Seguridad de TI. Planeación y Administración de Seguridad en TI"* UNAM CERT.

2. **KPMG,** Auditores Consultores Lida. Entendiendo la Administración de Riesgo Empresarial. Un Modelo Emergente para generar valor al Accionanista.

3. **LAZARO**, T Max. Seguridad de la Información. Oficina Nacional de Gobierno electrónico e informática.

4. **MURGUÍA,** Luis Miguel CISSP. Modelos de Seguridad de TI Arquitectura y Modelos de Seguridad Informática. UNAM CERT.

5. **InformationWeek México**. Los 13 CIO más prometedores de menos de 40 años. Pag. 8 y 10. Revista.

Capítulo 2

6. **APARICIO**, Fernando. Análisis y Gestión de Riesgos. 8/04/2005 First Conference Security Xperts.

7. **CANO,** Jeimy. Pautas y Recomendaciones para elaborar Políticas de Seguridad Informática.

8. **MURGUÍA,** Luis Miguel CISSP. ISMS Documentos básicos. Políticas y Planes de Contingencia. UNAM CERT.

9. **CompTIA.** Interoperabilidad y estándares abiertos: Guía para la clase Política Julio 2006.

10. **Universidad Nacional de Colombia**, Dirección Nacional de Informática y comunicaciones. Guía para elaboración de Políticas de Seguridad 2003.

Capítulo 4

11. **ACEITUNO,** Canal Vicente. Information Security Management Maturity Model ISM3 2.0. Creative Commons Attrib-Noderivs 3.0. License 2007.

12. **ACEITUNO,** Canal Vicente. Handbook. ISM3 2.0. Creative Commons Attrib-Noderivs 3.0. License 2007.

Mesografía

Capítulo 1

1. **MICROSOFT.** Más información acerca del sector TI. Fecha de creación el 13 de julio de 2001, disponible en: http://www.microsoft.com/spain/formacion/training/careers/learn.mspx. Consulta: 21-06-06

2. **CANO,** Martínez Jeimy José. Credenciales para investigadores forenses en informática. Certificaciones y entrenamiento. Fecha de creación septiembre del 2001, disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=804 Consulta: 21-06-06

3. **PRIETO**, Bozec Arturo. Seguridad informática. Disponible en: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=7 Consulta: 21-06-06

4. **REVISTA RED.** Seguridad Informática ¿Qué, porqué y para qué?. Fecha de creación noviembre del 2002, disponible en: http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm Consulta: 21-06-06

5. **EUROLOGIC.** Conceptos Básicos de Seguridad Informática. Fecha de creación 2005, disponible en: http://www.eurologic.es/conceptos/conbasics.htm Consulta: 21-06-06

6. **MOBILIZA.** Seguridad Informática. Fecha de creación septiembre del 2005, disponible en: http://www.mobiliza.net/Servicios/seguridad-Informatica.htm Consulta: 22-06-06

7. **ROBLE.** Seguridad Informática. Fecha de creación 2001, disponible en: http://personales.ciudad.com.ar/roble/seguridadinformatica.htm Consulta: 22-06-06

8. **ALERTA ANTIVIRUS.** Disponible en: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=9 Consulta: 22-06-06

9. **ALVAREZ**, Marañon Gonzalo. Fecha de creación 2000, disponible en: http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html Consulta: 22-06-06

10. **AUDITORÍA SISTEMAS**. Seguridad Informática. Disponible en: http://www.auditoriasistemas.com/seguridad_informatica.htm Consulta: 23-06-06.

11. **ESPINTIME**. Objetivos de seguridad. Fecha de creación 2005, disponible en: http://www.espintime.com/es/security/why_2.html Consulta: 23-06-06.

12. **MICROSOFT.** Glosario de seguridad. Disponible en: http://www.microsoft.com/latam/technet/seguridad/glosario/default.mspx Consulta: 23-06-06.

13. **ALERTA ANTIVIRUS.** La seguridad de la información. Disponible en: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=4&pagina=1 Consulta: 23-06-06.

14. **RUZ,** Miguel A. Los servicios de seguridad. Fecha de creación 2005, disponible en: http://www.delitosinformaticos.com/especial/seguridad/servicios.shtml Consulta: 23-06-06.

15. **SANTIAGO,** C. Claudia. ¿Qué es la seguridad informática?. Fecha de creación septiembre del 2005, disponible en: http://www.citel.oas.org/newsletter/2005/septiembre/seguridad_e.asp Consulta: 23-06-06.
16. **ORUÉ,** López Beatriz**.** Marcas de agua en el mundo real. Fecha de creación el 13 de marzo del 2002, disponible en: http://www.instisec.com/publico/impresora.asp?seccion=4&id=68 Consulta: 23-06-06.

17. **NOEL.** Clasificación y tipos de ataques contra sistemas de información. Fecha de creación 25 de marzo del 2001, disponible en: http://www.delitosinformaticos.com/seguridad/clasificacion.shtml Consulta: 23-06-06.

18. **LA RED,** Martinez David Luis. Seguridad de Linux. Fecha de creación del 2001, disponible en: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGLI200_archivos/seguridadfisica.htm Consulta: 23-06-06.

19. **TALENGS**, Oliag Sergio. Seguridad Física. Disponible en: http://www.uv.es/sto/cursos/icssu/html/ar01s04.html Consulta: 23-06-06.

20. **DEBIAN.** Seguridad Física. Fecha de creación 8 de mayo del 2005, disponible en: http://guadapeich.bitacoras.com/archivos/2005/05/08/seguridad-fisica Consulta: 23-06-06.

21. **ALMADELIA**, Prácticas delictivas a través del internet. Disponible en: http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap5.htm Consulta: 23-06-06.

Capítulo 2

22. **ESPIÑEIRA**. ROSI: el ROI de la Seguridad de la Información. Fecha de creación 13 de junio del 2006, disponible en: http://www.pc-news.com/detalle.asp?sid=&id=6&Ida=2480 Consulta: 21-06-06.

23. **ADAPTEPYME.** Glosario de términos del autodiagnóstico**.** Disponible en: http://www.adaptepyme.net/glosario.php Consulta: 21-06-06.

24. **MICROSOFT.** Guía de administración de riesgos de seguridad. Fecha de creación 15 de octubre del 2004, disponible en: http://www.microsoft.com/latam/technet/articulos/adminriesgos/srsgch02.mspx Consulta: 22-07-06.

25. **MINISTERIO DE ADIMINISTRACIONES PÚBLICAS.** Criterios de seguridad. Consejo Superior de Informática. Fecha de creación 24 de junio del 2004, disponible en: http://www.csi.map.es/csi/criterios/seguridad Consulta: 22-07-06.

26. **TOPETE,** Contreras Clemente ¿Sabes cómo debes clasificar la información?, Clemente Topete Contreras. Disponible en: http://microasist.com.mx/noticias/tp/ctctp210904.shtml Consulta: 22-07-06.

27. **PÉREZ,** Arbesú Lizzette. Cuando no se miden los riesgos. Fecha de creación 1 de septiembre del 2006, disponible en: http://www.bsecure.com.mx/articulos.php?id_sec=53&id_art=6393&num_page=180 Consulta: 02-09-06.
28. **CIO ESPAÑA.** Las empresas tenderán a contener su inversión en TI, según los analistas. Fecha de creación 10 de diciembre del 2005, disponible en: http://www.idg.es/CIO/mostrarArticulo.asp?id=172584&seccion=economia Consulta: 02-09-06.

29. **MICROSOFT.** Guía de administración de riesgos de seguridad. Fecha de creación 8 de mayo del 2005, disponible en: http://www.microsoft.com/latam/technet/articulos/adminriesgos/srsgch02.mspx Consulta: 02-09-06.

Capítulo 3

30. **BAÑUELOS,** José Luis. Con mejoras de control interno las empresas pequeñas pueden ser más eficientes. Fecha de creación 6 de abril del 2006, disponible en: http://portal.imcp.org.mx/content/view/2581/200/ Consulta: 29-11-06

31. **BAÑUELOS,** José Luis. La evaluación y autoevaluación del comité de auditoría. Fecha de creación 1 de septiembre del 2005, disponible en: http://portal.imcp.org.mx/content/view/758/196/ Consulta: 29-11-06

32. **MICROSOFT.** Grupo de pruebas de ataques e infiltraciones de Microsoft IT. Fecha de creación 17 de diciembre del 2004, disponible en: http://www.microsoft.com/spain/technet/recursos/articulos/attackandpenetest.mspx Consulta: 29-11-06

33. **STEALTH/ISS LLC.** Ley de Notificación de Violaciones de la Seguridad. Fecha de creación 2005, disponible en: http://www.stealth-iss.net/stealthllc/securityes/breach.html Consulta: 29-11-06

34. **THE FEDERAL RESERVE BOARD.** Leyes de mayor importancia para la protección del consumidor. Disponible en: http://www.federalreserve.gov/Pubs/complaints/leyes.htm Consulta: 29-11-06

35. **Practical Money Skills for Life.** Protección Federal de la confidencialidad. Fecha de creación: 2000, disponible en: http://practicalmoneyskills.com/spanish/at_home/consumers/identity/federal/gramm.php Consulta: 29-11-06

36. **LEXJURIS.** Ley Num. 369 del año 2000. Fecha de creación: 2000, disponible en: http://www.lexjuris.com/lexlex/Leyes2000/lex2000369.htm Consulta: 29-11-06

37. **TRUSTWAVE.** Servicios de conformidad de empresas. Disponible en: http://www.atwcorp.com/global/esp/enterprise.php Consulta: 29-11-06

38. **ONTRACK.** Adecuación a las leyes de protección de documentos. Fecha de creación: 2006, disponible en: http://www.ontrack.es/especial/leyes-documentos.aspx Consulta: 29-11-06

39. **KPMG.** Ley Sarbanes-Oxley. Fecha de creación: 2006, disponible en: http://www.kpmg.com.mx/gobiernocorporativo/html/rrr_sox.htm Consulta: 29-11-06

40. **BULLTEK.** Sarbanes-Oxley. Disponible en: http://www.bulltek.com/Spanish_Site/ISO%209000%20INTRODUCCION/ISO%209000-2000_Spanish/sarbanes_oxley_spanish/sarbanes_oxley_spanish.html Consulta: 29-11-06

41. **TECH FAQ.** Qué es la Ley Sarbanes-Oxley? Disponible en: http://www.tech-faq.com/lang/es/sarbanes-oxley.shtml Consulta: 29-11-06

42. **DATA SEC.** Sarbanes-Oxley e Informe COSO. Disponible en: http://www.datasec.com.uy/archivos/SARBANES_OXLEY_E_INFORME_COSO.pdf Consulta: 29-11-06

43. **BUSINESS OBJECTS.** Sobre la Ley Sarbanes-Oxley. Disponible en: http://www.latam.businessobjects.com/soluciones/empresariales/sarbanes_oxley_reporting.asp Consulta: 29-11-06

44. **HEALTH AND HUMAN SERVICES.** HIPAA. Fecha de creación 16 de febrero del 2006, disponible en: www.hhs.gov/ocr/hipaa/ Consulta: 29-11-06

45. **ASES.** Ley HIPAA y ASES. Fecha de creación 27 de junio del 2006, disponible en: http://www.gobierno.pr/ASES/HIPAA/LEYHIPAAASES.htm Consulta: 29-11-06

46. **MCAFEE.** Una guía práctica para cumplir niveles de conformidad. Disponible en: http://www.mcafee.com/mx/enterprise/security_insights/practical_guide_compliance.html Consulta: 29-11-06

47. **ADA.** Cobertura para los individuos elegibles de HIPAA. Fecha de creación: 2003, disponible en: http://www.diabetes.org/espanol/apoyolegales/hipaa.jsp Consulta: 29-11-06

48. **PARDEY**, Phillip. Están los Derechos de Propiedad Sofocando la Biotecnología en los Países en Desarrollo?. Fecha de creación: 2001, disponible en: http://www.ifpri.org/spanish/pubs/essays/ar2000_essay02sp.htm Consulta: 30-11-06

49. **Yoke,** Ling Chee. La batalla por los derechos de propiedad intelectual. Fecha de creación 13 de marzo del 2006, disponible en: http://www.redtercermundo.org.uy/texto_completo.php?id=2985 Consulta: 30-11-06

50. **BURRONE,** Esteban. Las normas técnicas, los derechos de propiedad intelectual (DPI) y el proceso de establecimiento de normas. Disponible en: http://www.wipo.int/sme/es/documents/ip_standards.htm Consulta: 30-11-06

51. **GRUPO ETC.** Propiedad intelectual y patentes. Disponible en: http://www.etcgroup.org/es/los_problemas/propiedad_intelectual_y_patentes.html Consulta: 30-11-06

52. **CINU.** Propiedad intelectual. Fecha de creación: 2006, disponible en: http://www.cinu.org.mx/temas/desarrollo/desecon/prop_intelec.htm Consulta: 30-11-06

53. **LAZARD,** Deborah. La protección de la tecnología a través de las patentes. Disponible en: http://whybiotech.com/mexico.asp?id=2707 Consulta: 30-11-06

54. **KPMG.** Componentes de control de acuerdo con COSO. Fecha de creación: 2006, disponible en: http://www.kpmg.com.mx/gobiernocorporativo/html/rrr_sox_coso.htm Consulta: 30-11-06

55. **PC-NEWS.** Las Tecnologías de Información y el Control Interno: socios para el cumplimiento de la Ley**.** Fecha de creación 19 de octubre del 2004, disponible en: http://www.pc-news.com/detalle.asp?sid=&id=6&Ida=1770 Consulta: 30-11-06

56. **CRUZ,** Daniel. ISO 17799: La gestión de la seguridad. Fecha de creación julio del 2003, disponible en: http://www.virusprot.com/Art41.htm Consulta: 30-11-06

57. **HERNANDO,** Sergio. La seguridad ligada al personal. Criterios ISO 17799. Fecha de creación 1 de marzo del 2006, disponible en: http://www.sahw.com/wp/archivos/2005/07/08/la-seguridad-ligada-al-personal-criterios-iso-17799/ Consulta: 30-11-06

58. **FINANCIAL TECH.** ISO/IEC 17799. Fecha de creación 7 de julio del 2005, disponible en: http://www.financialtech-mag.com/000_estructura/index.php?id=24&idb=43&ntt=2729&sec=14&vn=1 Consulta: 30-11-06

59. **INTECO.** MAGERIT. Fecha de creación 2 de noviembre del 2005, disponible en: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=3&pagina=0 Consulta: 04-12-06

60. **IAGP.** MAGERIT. Fecha de creación: 2006, disponible en: http://www.um.es/docencia/barzana/IAGP/Iagp5.html#BM8 Consulta: 04-12-06

61. **CAO,** Avellaneda Javier. Análisis y gestión de riesgos de la seguridad de los sistemas de la información. Fecha de creación 7 de marzo del 2005, disponible en: http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php Consulta: 04-12-06

62. **ESPIÑEIRA,** Nuevos estándares para la evaluación de riesgos. Fecha de creación 6 de junio del 2006, disponible en: http://www.pc-news.com/detalle.asp?ida=2470 Consulta: 06-12-06

63. **UNIVERSIDAD NACIONAL DE COLOMBIA**. ISO 17799. Disponible en: http://www.seguridad0.com/index.php?1e4f922838f4bd3f6145495d5fa08980&ID=1556 Consulta: 07-12-06

64. **CVEIRA.** El gran dibujo de los estándares de seguridad. Fecha de creación 8 de marzo del 2005, disponible en: http://www.deepzone.org/main/index.php?p=146 Consulta: 07-12-06

65. **BORGHELLO,** Cristian Seguridad Lógica. Disponible en: http://www.segu-info.com.ar/logica/seguridadlogica.htm Consulta: 07-12-06

66. **DEBENEDET,** Alejandro. COBIT: EL marco de Control para TI. Disponible en: http://www.exo.com.ar/exos/paginas/plantillas_contenido/seccion.asp?seccion=253&pagina=65&idnove=0 Consulta: 07-12-06

67. **LRQA.** Normas y Servicios, ISO 9001:2000. Fecha de creación 8 de mayo del 2005, disponible en: http://www.lrqaspain.com/essite/template.asp?name=esstandards_iso9001_2000 Consulta: 08-12-06

68. **UL.** Certificación de Sistemas de Gestión. ISO 9001:2000. Fecha de creación: 2005, disponible en: http://www.ul-mexico.com/management/es_ulla_management_quality_ISO9001.aspx Consulta: 08-12-06

69. **FERNANDEZ,** Pereda Héctor. ISO 9001 Norma de Calidad. Disponible en: http://www.buscarportal.com/articulos/iso_9001_gestion_calidad.html Consulta: 08-12-06

70. **VELAZQUEZ,** Andrés. Los mitos del British Standard 7799 y el ISO 17799. Disponible en: http://www.mattica.com/articulo_detalle.php?id=4 Consulta: 13-12-06

71. **BSECURE.** ¿Cumple o no cumple?. Fecha de creación 2 de marzo del 2005, disponible en: http://www.bsecure.com.mx/articulos.php?id_sec=51&id_art=5097&id_ejemplar=318 Consulta: 13-12-06

72. **MENDOZA.** ISO 17799. Fecha de creación 6de septiembre del 2004, disponible en: http://weblog.mendoza.edu.ar/jinformatico/archives/001780.html Consulta: 13-12-06

73. **SANTOS,** Pascual Efrén. Gestión de la Seguridad de la información. Disponible en: http://www.microsoft.com/spain/empresas/legal/gestion_seguridad.mspx Consulta: 13-12-06

74. **GRUPO CONSULTORIA.** Modelo de Capacidad y Madurez Integrado. Disponible en: http://www.grupoconsultoria.com.co/cmmi.htm Consulta: 13-12-06

75. **GRACIA,** JOAQUIN. CMMI. Fecha de creación 14 de agosto del 2005, disponible en: http://www.ingenierosoftware.com/calidad/cmm-cmmi.php Consulta: 13-12-06

76. **SINERGIT.** Qué es ITIL?. Disponible en: http://www.sinergit.com.do/sobre_itil.htm Consulta: 13-12-06

77. **CIO CONSULTORES.** ITIL El estándar de-facto para la Gestión de Servicios TI. Disponible en: http://www.cioconsultores.cl/Articulos/Art_ITIL.htm Consulta: 13-12-06

78. **DRUTA,** Enrique Gustavo. Actualización de la Norma ISO 17799:2005 y Creación de la ISO 27001:2005 Fecha de creación 24 de febrero del 2006, disponible en: http://seguridadit.blogspot.com/2006/02/mas-sobre-iso-1779927001.html Consulta: 13-12-06

79. **CSI.** Normas y estándares aplicables. Disponible en: http://www.csi.map.es/csi/silice/Segurd21.html Consulta: 13-12-06

80. **CMS.** ¿Qué es HIPAA? Disponible en: http://www.triples-med.org/webmedicare/hipaa/ Consulta: 13-12-06

81. **Aris**, Papathéodorou. Propiedad intelectual, copyright, patentes. Fecha de creación: 2001, disponible en: http://biblioweb.sindominio.net/telematica/aris-pi.html Consulta: 13-12-06

82. **SICE.** Derechos de Propiedad Intelectual. Disponible en: http://www.sice.oas.org/int_prop/nat_leg/Mexico/lipmexsa.asp#tit2cap2 Consulta: 13-12-06

83. **NUÑEZ,** Sandoval Alejandro. Fecha de creación febrero del 2005, disponible en: http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm Consulta: 13-12-06

84. **ACEITUNO,** Canal Vicente.Disponible en: www.ism3.com Consulta: 11-01-08

85. **CAO,** Avellaneda Javier. ISO/IEC 15408: los Criterios Comunes.Disponible en: http://www.revistasic.com/revista46/criterios_46.htm Consulta: 11-01-08

86. **ISO2700.** ISO 2700. Disponible en: http://www.iso27000.es/doc_iso27000_all.htm Consulta: 11-01-08

Capítulo 4

87. **ACEITUNO,** Canal Vicente.Disponible en: www.ism3.com Consulta: 13-12-07