UNIVERSIDAD DE CHILE
FACULTAD DE ECONOMIA Y NEGOCIOS
ESCUELA DE SISTEMAS DE INFORMACION Y AUDITORIA

"ESTANDARES PARA LA SEGURIDAD DE INFORMACIÓN CON TECNOLOGIAS DE INFORMACIÓN"

Seminario para optar al titulo de Ingeniero en Información y Control de Gestión

Participantes: Johanna Medina Iriarte

Profesor Guía: Raúl Suárez

Otoño 2006

A mi Madre……

Agradecimientos

A mi Madre, que en todo momento ha estado conmigo, ha sido el apoyo fundamental en mi vida y mi carrera universitaria, gracias a ella soy lo que soy, como mujer y como profesional. Por darme las herramientas necesarias para mi completo desarrollo.

A mi familia en general, tíos y primos, en especial a mis Abuelos y Hermano, por su comprensión y motivación.

A mi pololito que me ha dado la motivación y fuerza para terminar mi carrera, por su apoyo incondicional.

A mi profesor guía don Raúl Suárez agradezco su disposición de haber guiado desde un principio esta investigación, por sus sugerencias y alcances.

A mis amigos todos por su gran "Paciencia"

Índice

Introducción

En toda organización actual, la seguridad de la información a comenzado a tomar un lugar muy importante, en cuanto a como se gestiona la Tecnología de Información, y se ha convertido en un elemento fundamentalmente considerado en toda estrategia de negocio con miras a lograr metas importantes, tanto como a corto, mediano y largo plazo.

En consecuencia, las organizaciones experimentan la necesidad de definir estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle mayor resguardo a la información, y al mismo tiempo no obstáculos para adaptarse a los continuos cambios de la organización como consecuencia de las exigencias del mercado.

Tal necesidad ha impulsado el énfasis en el planteamiento de nuevos paradigmas de la administración del entorno de TI basada en políticas y procedimientos. Esto ha llevado a la creación de estándares, códigos de buenas prácticas, desarrollos de políticas, etc., con motivo de resguardar uno de los activos más valiosos de las organizaciones como es la información.

Con la apertura de las empresas al mundo de Internet, se han abierto oportunidades de creación de nuevos negocios, tanto en chile como mundialmente. Por lo tanto actualmente es un tema prioritario para las empresas el resguardo de su información, ya que es un tema que abarca a las organizaciones desde las tareas más sencillas como a temas más complejos relacionados con el negocio y su supervivencia como organización.

Además, en una economía globalizada, como ocurre actualmente, donde los países y organizaciones están relacionados, también surge la necesidad de unificar criterios en

cuanto a la seguridad, por lo que necesariamente surge la necesidad de certificar que las condiciones de seguridad son optimas, tanto para las empresas como parar sus clientes.

El presente trabajo esta orientado principalmente, a enumerar y desarrollar algunas políticas y estándares sobre seguridad de la información con tecnologías de información, que están presentes actualmente.

Capitulo I

Importancia de la seguridad en los sistemas de información

1.1 Introducción

Toda organización requiere para su funcionamiento ciertas condiciones básicas que permitan facilidad para la realización de las tareas de una forma más efectiva y eficientes.

En las organizaciones se produce gran cantidad de información, que cualquier gerente que no cuente con sistemas bien diseñados de información, seria muy difícil tomar las decisiones más adecuadas y oportunas para resolver los problemas que se le puedan presentar.

Los sistemas de información constituyen una herramienta de suma importancia para realizar las funciones de cualquier organización por muy pequeña que esta sea, ya que este permite recopilar, clasificar, procesar interpretar y resumir cantidades de datos que permitirán la toma eficiente de decisiones.

Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una

plataforma de información necesaria para la toma de decisiones y, lo más importante, su implementación logra ventajas competitivas o reducir la ventaja de los rivales.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros.

Los componentes anteriores conforman los protagonistas del desarrollo informático en una organización, tanto para su desarrollo como para su aplicación, además se reconoce que las tecnologías de la información constituyen el núcleo central de una transformación multidimensional que experimenta la economía y la sociedad; de aquí lo importante que es el estudio y dominio de las influencias que tal transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar.

Dentro de las tecnologías de la información también debemos contemplar algunos conceptos y/o metodologías que merecen estar clasificadas como de alto impacto, ya sea para nuestra organización, el individuo o la sociedad misma.

1.2 La información como recurso de las organizaciones

Desde hace ya algunos años las organizaciones han reconocido la importancia de administrar los principales recursos como la mano de obra y las materias primas.

La información se ha colocado en un buen lugar como uno de los principales recursos que poseen las empresas actualmente. Los entes que se encargan de las tomas de decisiones han comenzado a comprender que la información no es sólo un subproducto

de la conducción empresarial, sino que a la vez alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de éstos.

Si deseamos maximizar la utilidad que posee nuestra información, el negocio la debe manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes. Los administradores deben comprender de manera general que hay costos asociados con la producción, distribución, seguridad, almacenamiento y recuperación de toda la información que es manejada en la organización. Aunque la información se encuentra a nuestro alrededor, debemos saber que ésta no es gratis, y su uso es estrictamente estratégico para posicionar de forma ventajosa la empresa dentro de un negocio.

La fácil disponibilidad que poseen las computadoras y las tecnologías de información en general, han creado una revolución informática en la sociedad y de forma particular en los negocios. El manejo de información generada por computadora difiere en forma significativa del manejo de datos producidos manualmente.

La Seguridad de la Información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la Seguridad de la Información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

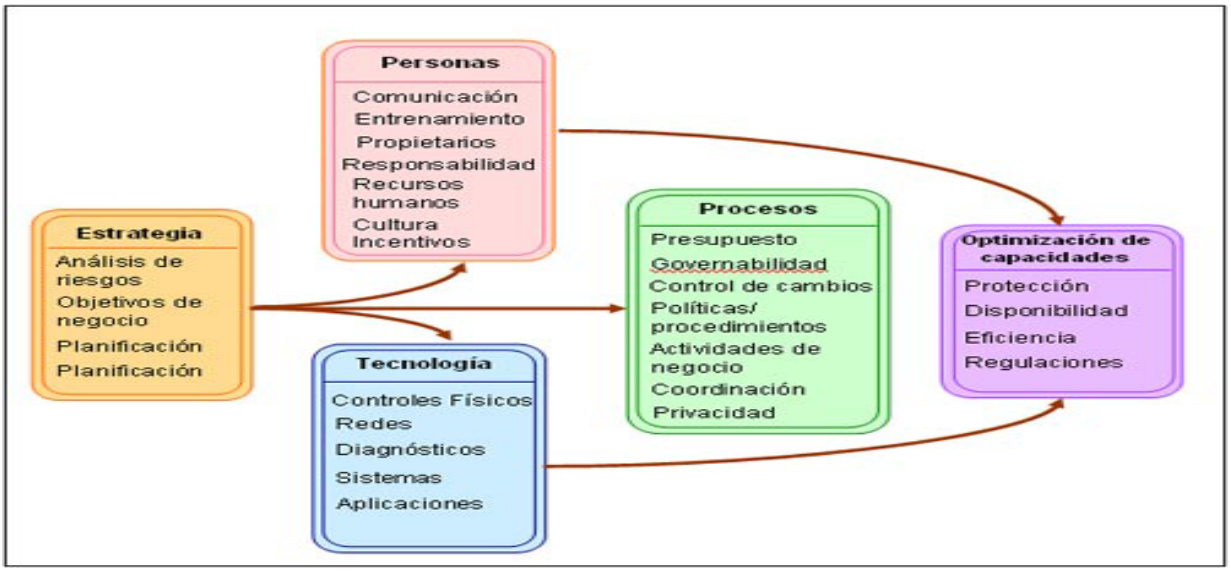
La Seguridad de la Información es otro proceso estratégico del negocio ya que al lograr el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información en línea con los objetivos de negocio, se estarán optimizando substancialmente las operaciones. La noción de Seguridad de la Información como un

habilitador de negocios es hoy día un concepto esencial para las organizaciones de cualquier sector industrial.

Como un proceso estratégico, la Seguridad de la Información pudiera estar enfocada en proteger los activos de información de una organización contra pérdidas o uso indebido, o focalizada a brindar acceso a los activos de información apoyando los objetivos de negocio. Uniendo estos dos conceptos – seguridad como "Protección" y seguridad como "Habilitador de Accesos" – se define de manera integral un nuevo enfoque de Seguridad de la Información en las organizaciones.

La Seguridad de la Información hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. (Ver Figura 1). Si no se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos, y ante la ausencia de personal que es capacitado para la gestión del proceso, la inversión en tecnología solamente no es más que una pérdida de dinero. Este concepto de Seguridad de la Información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio.

A medida que el rol de Seguridad de la Información evoluciona, los directivos y ejecutivos de negocio reconocen que éste es sin duda el primer paso en la relación entre la organización, sus clientes, socios de negocio, proveedores y empleados. En este sentido, la Seguridad de la Información acarrea enormes implicaciones para las organizaciones debido a que la confianza es la base para el intercambio, y su ausencia es una buena razón para hacer negocios con la competencia.



1.3 Definición de Sistema de Información

Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware). Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado"

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

- **Entrada de información:** proceso en el cual el sistema toma los datos que requiere para procesar la información, Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa

por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfases automáticas.

Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de diskette, los códigos de barras, los escáners, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

- **Almacenamiento de información**: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).

- **Procesamiento de la información**: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

- **Salida de información:** La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo.

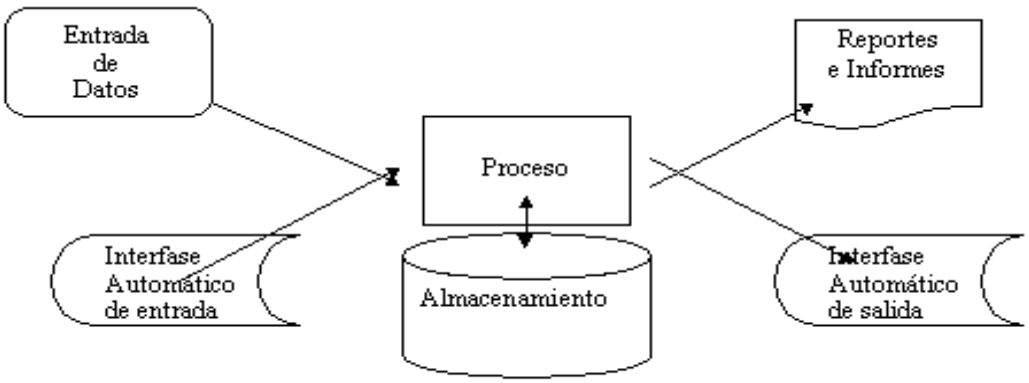
1.3.1 Tipos y usos de los sistemas de información

Los Sistemas de Información cumplen tres objetivos básicos dentro de las organizaciones:

1. Automatización de procesos operativos.

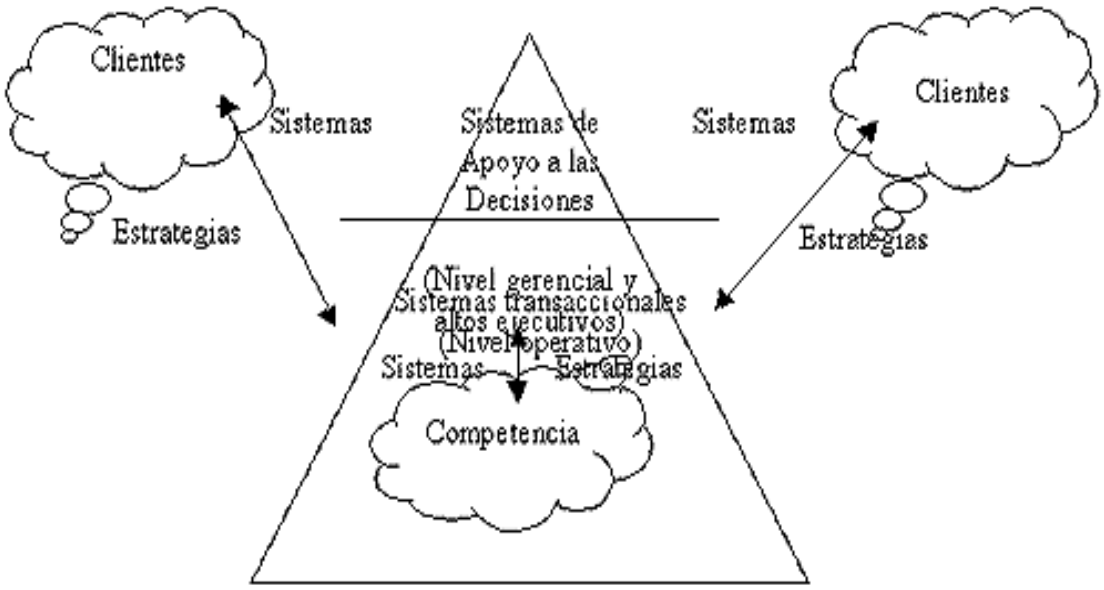
2. Proporcionar información que sirva de apoyo al proceso de toma de decisiones.

3. Lograr ventajas competitivas a través de su implantación y uso.



Los Sistemas de Información que logran la automatización de procesos operativos dentro de una organización, son llamados frecuentemente Sistemas Transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc. Por otra parte, los Sistemas de Información que apoyan el proceso de toma de decisiones son los Sistemas de Soporte a la Toma de Decisiones, Sistemas para la Toma de Decisión de Grupo, Sistemas Expertos de Soporte a la Toma de Decisiones y Sistema de Información para Ejecutivos. El tercer tipo de sistema, de acuerdo con su uso u objetivos que cumplen, es el de los Sistemas Estratégicos, los

cuales se desarrollan en las organizaciones con el fin de lograr ventajas competitivas, a través del uso de la tecnología de información.



A continuación se mencionan las principales características de estos tipos de Sistemas de Información.

1.3.1.1 Sistemas Transaccionales.

Sus principales características son:

- A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas de la organización.

- Con frecuencia son el primer tipo de Sistemas de Información que se implanta en las organizaciones. Se empieza apoyando las tareas a nivel operativo de la organización.

- Son intensivos en entrada y salid de información; sus cálculos y procesos suelen ser simples y poco sofisticados.

- Tienen la propiedad de ser recolectores de información, es decir, a través de estos sistemas se cargan las grandes bases de información para su explotación posterior.

- Son fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.

1.3.1.2 Sistemas de Apoyo de las Decisiones.

Las principales características de estos son:

- Suelen introducirse después de haber implantado los Sistemas Transaccionales más relevantes de la empresa, ya que estos últimos constituyen su plataforma de información.

- La información que generan sirve de apoyo a los mandos intermedios y a la alta administración en el proceso de toma de decisiones.

- Suelen ser intensivos en cálculos y escasos en entradas y salidas de información. Así, por ejemplo, un modelo de planeación financiera requiere poca información de entrada, genera poca información como resultado, pero puede realizar muchos cálculos durante su proceso.

- No suelen ahorrar mano de obra. Debido a ello, la justificación económica para el desarrollo de estos sistemas es difícil, ya que no se conocen los ingresos del proyecto de inversión.

- Suelen ser Sistemas de Información interactivos y amigables, con altos estándares de diseño gráfico y visual, ya que están dirigidos al usuario final.

- Apoyan la toma de decisiones que, por su misma naturaleza son repetitivos y de decisiones no estructuradas que no suelen repetirse. Por ejemplo, un Sistema de Compra de Materiales que indique cuándo debe hacerse un pedido al proveedor o un Sistema de Simulación de Negocios que apoye la decisión de introducir un nuevo producto al mercado.

- Estos sistemas pueden ser desarrollados directamente por el usuario final sin la participación operativa de los analistas y programadores del área de informática.

- Este tipo de sistemas puede incluir la programación de la producción, compra de materiales, flujo de fondos, proyecciones financieras, modelos de simulación de negocios, modelos de inventarios, etc.

1.3.1.3 Sistemas Estratégicos.

Sus principales características son:

- Su función primordial no es apoyar la automatización de procesos operativos ni proporcionar información para apoyar la toma de decisiones.

- Suelen desarrollarse in house, es decir, dentro de la organización, por lo tanto no pueden adaptarse fácilmente a paquetes disponibles en el mercado.

- Típicamente su forma de desarrollo es a base de incrementos y a través de su evolución dentro de la organización. Se inicia con un proceso o función en particular y a partir de ahí se van agregando nuevas funciones o procesos.

- Su función es lograr ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores. En este contexto, los Sistema Estratégicos son creadores de barreras de entrada al negocio. Por ejemplo, el uso de cajeros automáticos en los bancos en un Sistema Estratégico, ya que brinda ventaja sobre un banco que no posee tal servicio. Si un banco nuevo decide abrir su puerta al público, tendrá que dar este servicio para tener un nivel similar al de sus competidores.

- Apoyan el proceso de innovación de productos y proceso dentro de la empresa debido a que buscan ventajas respecto a los competidores y una forma de hacerlo en innovando o creando productos y procesos.

Un ejemplo de estos Sistemas de Información dentro de la empresa puede ser un sistema MRP (Manufacturing Resoure Planning) enfocado a reducir sustancialmente el desperdicio en el proceso productivo, o bien, un Centro de Información que proporcione todo tipo de información; como situación de créditos, embarques, tiempos de entrega,

etc. En este contexto los ejemplos anteriores constituyen un Sistema de Información Estratégico si y sólo sí, apoyan o dan forma a la estructura competitiva de la empresa.

Por último, es importante aclarar que algunos autores consideran un cuarto tipo de sistemas de información denominado Sistemas Personales de Información, el cual está enfocado a incrementar la productividad de sus usuarios.

1.3.2 Importancia de los sistemas de Información

Cuando muchas personas se preguntan por qué estudiar sobre los sistemas de información, es lo mismo que preguntar por qué debería estudiar alguien contabilidad, finanzas, gestión de operaciones, marketing, administración de recursos humanos o cualquier otra función empresarial importante. Lo que si se puede asegurar es que muchas empresas y organizaciones tienen éxitos en sus objetivos por la implantación y uso de los Sistemas de Información. Lo importante es tener una comprensión básica de los sistemas de información para entender cualquier otra área funcional en la empresa, por eso es importante también, tener una cultura informática en nuestras organizaciones que permitan y den las condiciones necesarias para que los sistemas de información logren los objetivos citados anteriormente. Muchas veces las organizaciones no han entrado en la etapa de cambio hacía la era de la información sin saber que es un riesgo muy grande de fracaso debido a las amenazas del mercado y su incapacidad de competir, por ejemplo, las TI que se basan en Internet se están convirtiendo rápidamente en un ingrediente necesario par el éxito empresarial en el entorno global y dinámico de hoy.

Por lo tanto, la administración apropiada de los sistemas de información es un desafío importante para los gerentes. Así la función de los SI representa:

- Un área funcional principal dentro de la empresa, que es tan importante para el éxito empresarial como las funciones de contabilidad, finanzas, administración de operaciones, marketing, y administración de recursos humanos.

- Una colaboración importante para le eficiencia operacional, la productividad y la moral del empleado, y el servicio y satisfacción del cliente.

- Una fuente importante de información y respaldo importante para la toma de decisiones efectivas por parte de los gerentes.

- Un ingrediente importante para el desarrollo de productos y servicios competitivos que den a las organizaciones una ventaja estratégica en el mercado global.

- Una oportunidad profesional esencial, dinámica y retadora para millones de hombres y mujeres

1.3.3 Seguridad en los sistemas de información

Las medidas de seguridad, tienen como objetivo principal preservar la integridad, disponibilidad, confiabilidad de la información, para lograr estos objetivos, está la:

- **Seguridad preventiva** que reduce la probabilidad de ocurrencia de eventos no deseados y reduce las consecuencias en caso de llegar a ocurrir dicho evento, que puede ocurrir a pesar de las medidas preventivas.

- **Seguridad reactiva** que se activa una vez ocurrido el evento no deseado, tiene como objetivo estructurar la organización para minimizar las consecuencias de lo

ocurrido y permitir enfrentar el presente y futuro de la mejor forma posible, a pesar de lo ocurrido.

La seguridad no es un proyecto, es un proceso continuo, es necesario:

- **Evaluar** (cuál es la situación actual),
- **Diseñar** (dónde necesitamos estar),
- **Implementar** (cómo llegamos desde donde estamos hacia adonde necesitamos estar)
- **Administrar y Soportar** (cómo nos mantenemos y mejoramos),

Todo lo anterior dentro de **políticas, estándares y normas de seguridad** y la correspondiente capacitación, en la actualidad existe el hackeo ético.

La seguridad puede ser en base a equipos propios o no, o en base a un servicio local o remoto, es decir, se puede administrar mediante web, en la actualidad existe el http y el https, las organizaciones dedicadas a seguridad, ofrecen los servicios de seguridad como un ASP, hacen hasta respaldos en forma remota y los resguardan.

En seguridad se debe cubrir:

- la **seguridad perimetral** (alámbrica e inalámbrica), debe cubrir de extremo a extremo
- **de contenido** (de datos y de software, en particular en el correo electrónico, en que a veces se burlan controles al usar zip, hay sw de seguridad que identifican y analizan archivos .zip),

- de identidad y
- del puesto de trabajo.
- debe implementarse con equipos de alta disponibilidad.

La tendencia en seguridad es: a dispositivo específico (appliances), móvil, biométrica, certificado electrónico, firewall personal, antivirus en red.

En el caso específico de seguridad en acceso remoto para clientes inalámbricos, clientless (necesario para teletrabajo y e-learning), tendencia a conectividad móvil, la

seguridad no es barrera, es a veces la llave del negocio, el problema de este acceso remoto es la diversidad de dispositivos, redes, protocolos, etc., lo anterior es porque hoy en día, la conectividad es desde cualquier parte, a cualquier hora, con cualquier acceso y cualquier dispositivo, las opciones son instalar software de seguridad en cada equipo lo cual es lento y largo, es mas conveniente instalarlo en los servidores y dar acceso central con balanceo de carga.

En conexión inalámbrica, (Ej.: wi-fi, wlan), la seguridad física no es suficiente, pues el vecindario es parte de la red, al hacer roaming dicha seguridad puede cambiar.

Ante un ataque, cuyas etapas son: previo al ataque, durante y después; el antiataque debe ser de prevención, no sirve de tipo de correctivo (ej.: saber que la empresa o el equipo fue atacado ayer), algunos equipamientos permiten que la administración de seguridad en estas plataformas se pueda hacer en forma centralizada,

En términos de seguridad, de la password se pasó a la VPN, después a la SSL-VPN y ahora está IPW (Instant Private Web), que corresponde a la autentificación remota, vía token que puede ser instalado en el puerto USB.

Para TI existen estos dos tipos de seguridad bastantes reconocibles, los cuales deben estar sujetos a un análisis costo beneficio antes de implementarlos, algunas de las medidas de seguridad son:

1.3.3.1 Tipos de seguridad en sistemas de información

1.3.3.1.1 Seguridad Física de tipo preventivo

Se tiene dentro de la seguridad física, distintos aspectos que pueden brindar seguridad tanto a las personas como a los equipamientos, además de la continuidad operacional. Algunos de estos elementos se mencionan a continuación:

- **Accesos Físicos**

Existen distintos controles físicos como:

- Guardia o portero, que significaría la primera barrera de seguridad de la empresa.

- Una segunda barrera serían tarjetas de visitas o magnéticas, en que indique a que piso se dirigen y les permita el acceso solamente al piso o sección indicada.

- Determinar zonas con accesos restringidos.

- Contar con circuitos cerrados de televisión (es necesario analizar dónde y cuántas cámaras de televisión instalar y qué y cuánto se grabará de lo que las cámaras filmen).

Las medidas de seguridad señaladas, siempre están restringidas por la cantidad de recursos monetarios que se dispongan, debiéndose realizar un análisis inversión v/s protección. Mientras la seguridad sea rentable, se invierte.

- **Equipos de Prevención**

Como prevención, existen distintos elementos e instalaciones que cumplen con estos objetivos, especialmente para prevenir incendios, por ejemplo:

- Extintores, se debe efectuar una planificación con respecto a la cantidad de extintores que se van a adquirir, como será la distribución, de que tipo (por ejemplo, especiales de gas para incendio en equipos de TI), tamaño, dado que los extintores tienen fecha de vencimiento, es necesaria una planificación logística de cuántos llevar a renovarse o llenarse y cuántos dejar en la empresa, etc.

- Detectores de humo, los cuales dan aviso por una concentración de humo superior a la permitida. Estos detectores se deben revisar cada cierto tiempo, además se pueden regular, según el sector en que están colocados. Deben ser instalados en altura (por las condiciones del humo, que siempre tiende a subir) y por gente capacitada.

- Detectores de gas, al igual que los de humo, se deben regular y revisar por gente capacitada. Su instalación debe ser a baja altura, ya que los gases suelen ser más pesados que el oxígeno, por lo que se acumulan a nivel del suelo.

- Mangueras y red seca. La red seca es común en edificios, son cañerías que van sin agua y se llenan en caso de incendio distribuyendo agua por todo el edificio. Por lo general, son de uso exclusivo de bomberos.

    - Sprinkler o rociadores. Dispositivos que se instalan y se accionan generalmente por temperatura, pueden ser de agua o de gas antifuego (como los extintores). En este tipo de

dispositivos también debe decidirse cuántos instalar, dónde, de que tipo, etc. y su instalación debe ser efectuada por personal especializado.

Además de la prevención de incendios, también se debe prevenir de otros tipos de siniestros como inundaciones, robos, terremotos, tormentas, etc. Para esto se deberá contar con el equipamiento e instalaciones especialmente adecuadas para disminuir las probabilidades de ocurrencia o disminución de las consecuencias, lógicamente de acuerdo a los recursos con que la empresa disponga y su análisis de costo/beneficio.

Ejemplos:

*Instalaciones para una adecuada canalización de las aguas lluvias en los edificios.

*Tecnología antisísmica.

- **UPS (Uninterrupted Power System)**

Son baterías de duración limitada, con las cuales se puede disponer de energía eléctrica en caso de corte del suministro, permitiendo continuidad y un cierre normal de los sistemas. El tamaño de la UPS depende del tiempo que desee usar, consumo de energía del equipo, etc., con esto en mente, puede llegarse a determinar la conveniencia económica y técnica de tener UPS.

Otra alternativa son los equipos moto-generadores o grupos electrógenos que comienzan a funcionar una vez que la UPS se agota. Esto es necesario o más útil cuando se trata de aplicaciones críticas. El inconveniente de estos motores es principalmente la inestabilidad de energía que presentan, por lo que es necesario combinarlo con un

estabilizador de voltaje. También requiere un análisis costo/beneficio, el valor de este tipo de equipos depende del consumo de energía de los equipos conectados a él.

- **Vías de Evacuación**

Es necesario capacitar y entrenar a la gente sobre cuales son las vías de escape, de manera que estas sean expeditas y se llegue en el menor tiempo posible a un punto de encuentro o de seguridad definido. La ruta debe ser segura en todo el trayecto y no debe entorpecer el flujo de quienes la están usando. En el punto de encuentro se debe efectuar un proceso de revisión y conteo para determinar si están todas las personas que debieran estar.

Todo lo anterior requiere de la debida y constante capacitación de las personas, tanto en cómo proceder ante un evento no deseado, como en el respectivo apoyo a las decisiones ante la información que los dispositivos de prevención entreguen.

1.3.3.1.2 Seguridad Lógica de tipo preventivo

En algunos aspectos la seguridad lógica imita a la seguridad física, lo cual no siempre es conveniente.

A continuación se describen algunas medidas de seguridad lógicas, que actúan en segundo nivel, es decir, después de las medidas de tipo físico:

- **Perfiles de Accesos**

Implica el uso de ID y password. Existen distintos niveles de control, los cuales son:

- **Nivel 0**: A nivel de Sistema Operativo. Todos los sistemas operativos lo traen, sólo hay que activarlo. Pide identificación y palabra clave

- **Nivel 1**: Se fijan privilegios, que es lo que se puede hacer. Los privilegios son:

**Read Only*: sólo lectura, no permite la modificación de la información.

**Modify*: permite a ciertos usuarios modificar la información y lo permitido en el privilegio anterior.

**Delete*: facultad de ciertos usuarios para borrar información existente y lo permitido en el privilegio anterior.

**Create*: máximo privilegio existente, crear archivos y lo permitido en el privilegio anterior.

- **Nivel 2**: Tiene relación con los menú de aplicaciones. Funciona sólo si el técnico lo activa. Hasta este nivel se maneja por el sistema operativo. Determina a qué aplicaciones tiene acceso el usuario.

- **Nivel 3**: corresponde a colocar protectores de pantalla con palabra clave que se activan en un determinado tiempo de inactividad del usuario y para volver a activar las aplicaciones se debe digitar la palabra clave correspondiente.

- **Nivel 4**: De aquí en adelante, los niveles son manejados por las aplicaciones. Existe un menú de opciones. Este se debe crear o instalar durante el diseño físico del sistema o verificarlo cuando se va a comprar el software. Cada aplicación, dependiendo de la misma y/o del usuario, puede pedir clave de acceso, como el nivel 0 anterior, pero sólo para dar acceso a la aplicación.

- **Nivel 5:** Permite definir acceso a funcionalidades dentro de la aplicación, a ciertos datos de la aplicación, etc. Y así en adelante.

- **Nivel 6**: Este nivel a diferencia de los anteriores no controla acceso, sino que corresponde a guardar el registro de los cambios hechos con los datos, para efectos de apoyar un futuro análisis en caso de problemas o anular el cambio y volver a como estaban los datos antes del cambio. Esto utiliza espacio de almacenamiento. Es necesario definir cuánta historia se va a almacenar.

- **Nivel 7**: Al igual que el nivel anterior, registra información, en este caso lo que se almacena es la identificación de quién efectuó cambios en los datos. Esto utiliza espacio de almacenamiento. Es necesario definir cuánta historia se va a almacenar.

Cada uno de los niveles de seguridad implica un uso de recursos de CPU, RAM, etc, que degrada los tiempos de respuesta, por lo que es necesario considerar este factor al evaluar la implementación de seguridad lógica.

Se debe verificar todos los niveles que la aplicación o sistema requiere. Lo básico es llegar al nivel 2, pero es necesario definir hasta que nivel implementar cuando se trabaja en e-commerce.

Adicional a lo anterior existe una medida de seguridad complementaria, consiste en el control de inactividad del usuario, es decir, transcurrido un determinado período de tiempo en que el usuario no ha efectuado actividad en el equipo, el sistema lo desconecta, exigiendo una reconexión, como al inicio de la conexión perdida.

- **Administración de Password**

La administración de password o claves, comprende una serie de acciones tanto de construcción de las mismas, como también del control de éstas, de manera de

imposibilitar el acceso al sistema, de personas no autorizadas. Por lo general, no se puede normar la construcción de una password, dado que sería muy fácil descubrirla, sólo se puede decir que se utilice la mayor cantidad de caracteres posibles, mezclando caracteres de letras, números y signos. No usar algo fácil de adivinar (nombre propio, fecha de nacimiento, etc.), para lo cual existen como apoyo algunos mecanismos que permiten generar claves aleatorias, que son más seguras. También puede existir frases de paso (privadas), que funcionan en caso de olvido de la clave. Se debe controlar la forma de distribución de claves, para evitar que sean interceptadas. Debe cuidarse los medios en que se almacenan las claves, ya sean en papel, algún medio magnético, etc. Se debe cambiar periódicamente (el tiempo de vida de las claves no debe ser indefinida), de acuerdo a los privilegios que tenga el usuario, ya que con periodos largos de vida, se hace más probable la captura o el descubrimiento de la clave. Al acceder a los sistemas, se debe permitir un máximo de intentos fallidos de digitar la clave o password, una vez cumplidos dichos intentos se debe bloquear el acceso y avisar de esta anomalía. Por último, también se debe tener un historial de password para no repetirlas y fijar procedimientos para la destrucción de claves.

Para los accesos remotos, se crean los Calling Back. Esto se hace entregando al usuario que viaja, un dispositivo de password creadas, mientras que el usuario debe entregar un listado de todos los teléfonos en donde se le puede contactar. El dispositivo va entregando una password cada vez que el usuario necesite conectarse, sólo tiene que llamar a la empresa solicitando contactarse y el software establecerá el contacto llamando de vuelta.

Adicionalmente existe otro mecanismo para el acceso remoto, muy usado para no tener tanta dependencia de un lugar físico, como en el caso anterior. Este mecanismo se denomina password de una vida y consiste en que la persona que viaja lleva consigo un dispositivo que al activarlo genera una password, coordinado con el equipo al cual se va

a conectar para que genera la misa clave y permita el acceso, esta clave sirve para conectarse una sola vez, si la persona se desconecta, al reconectarse debe recurrir nuevamente al dispositivo para que le genere una nueva password.

- **Encriptación**

Algoritmo usado para cifrar datos de forma tal que al ser enviados, si éstos son interceptados, sean indescifrables para cualquier otra persona que no sea el destinatario, que es quien tiene el mismo algoritmo para descifrar el mensaje. La encriptación puede ser variable o dinámica.

Al encriptar en letras se tiene una alta seguridad. Es preferible no usar palabras palíndromes (salas, anilina, radar, reconocer, etc.), ya que ayudan a desencriptar los mensajes enviados.

La idea inicial es que se reduzca al mínimo la probabilidad de que un hacker acceda a la red, no obstante dado que es posible que acceda a la red, para prevenir que pueda leer un mensaje, es que se envían encriptados, adicionalmente se puede almacenar datos encriptados, de hecho las claves o password se almacenan encriptadas.

La encriptación complementa a otras medidas de seguridad. El principio de la encriptación es impedir el descifrado del dato (excepto si se posee el algoritmo de encriptación), no obstante con las nuevas técnicas de análisis de encriptación efectuadas por medio de software, lo anterior no es posible, luego lo que se persigue al encriptar el buscar un algoritmo y combinación de posibilidades lo mas alta posible, de forma tal que su descifrado demande mucho tiempo (años), aún usando software de apoyo.

- **Protocolos de Seguridad**

Entre los protocolos de seguridad que son más avanzados tecnológicamente, están:

- **SSL**: Secure Socket Layer, conocido como servidor seguro, es el primer protocolo o sistema de seguridad de pagos virtuales que se lanzó al mercado y el más extendido en la actualidad en el mundo (muy utilizado para e-commerce). Encripta la información confidencial mientras ésta viaja por la red (mediante el sistema de cifrado RSA) y sólo puede ser desencriptada por el servidor destino. SSL garantiza privacidad de los datos transmitidos por la red.

-SET: Secure Electronic Transaction, aplicación del sistema PKI desarrollado por Master Card, IBM y Visa para autentificar a los titulares de las tarjetas de crédito en las transacciones en línea. El gran avance frente al SSL es que garantiza el no repudio (negación por parte del emisor a reconocer el envío de información). Garantiza la confidencialidad de la información, la integridad del mensaje y autentifica la legitimidad de las entidades o personas que participan en una transacción.

- **Firmas Digitales**

La ley se dictó el 12 de octubre, Chile fue el sexto país con firma electrónica, no obstante en los otros países no funciona. En Chile no elimina el notario, en otros países los eliminó. En Chile es la ley 19.799. Una firma electrónica es un sonido, símbolo o proceso electrónico, que permita al receptor de un documento electrónico identificar formalmente al autor, la firma electrónica debe obtenerse por medio de un certificado de firma electrónica, que corresponde al documento que entrega la entidad certificadora, a quien adquiere una firma electrónica, dicho certificado y en consecuencia la firma

electrónica tienen una validez limitada de tiempo. La entidad certificadora requiere estar acreditada para efectuar dicha función. Hay firma electrónica avanzada, (es la que tiene validez jurídica, ante un tribunal por ejemplo) solo la puede otorgar un prestador acreditado. En el ámbito privado, la institucionalidad la rige la Subsecretaria de Economía. Las normas técnicas asociadas dependen del concepto, por ejemplo hay para seguridad, para estructura de certificados, para repositorio de información (que no siempre conversan entre si).

Una firma digital es un bloque de caracteres que acompaña a un documento (o archivo), acreditando quien es su autor (autentificación) y que no ha existido ninguna manipulación posterior de los datos (integridad). La firma digital es única para cada documento, a diferencia de la firma manual que es la misma siempre.

Para firmar un documento digital, el autor utiliza su propia clave secreta, a la que solo él tiene acceso, lo que impide que pueda negar su autoría (no repudio). De esta forma, el autor queda vinculado al documento que firma.

Cualquier persona puede verificar la validez de una firma, si dispone de la clave pública del autor.

Para la realización de una firma digital, el software del firmante aplica un algoritmo Hash (revoltijo) sobre el texto a firmar, obteniendo un extracto de longitud fija y absolutamente específico para cada mensaje (un mínimo cambio en el mensaje produce un extracto completamente diferente). Los algoritmos Hash más utilizados son MD5 y SHA-1. De acuerdo al algoritmo que se utilice, el extracto toma una longitud de entre 128 y 160 bits. Este extracto se somete a un cifrado mediante la clave secreta del autor, previa petición de contraseña. El extracto cifrado constituye la firma digital y se añade al final del mensaje (o en un archivo adherido a él).

Utilizando la clave pública, el software receptor descifra el extracto cifrado que constituye la firma digital, obteniéndose un bloque de caracteres. Luego se calcula el extracto Hash que corresponde al texto del mensaje y se compara con el bloque de

caracteres obtenidos anteriormente, si son exactamente iguales, la firma se considera válida.

- **PKI (Public Key Indicator)**

Infraestructura de clave pública, sistema de certificación digital diseñado para garantizar la seguridad de cualquier intercambio económico o de documentos en la red. Para su funcionamiento, el usuario debe tener una clave privada que se guarda en una tarjeta inteligente. El servidor posee otra clave pública que le autentifica en cualquier transacción económica o intercambio documental. El árbitro es una Autoridad de Certificación (AC) que emite un certificado válido durante un periodo preestablecido (renovable). Cualquier entidad pública o privada podrá constituirse como AC en libre competencia.

La posesión de la clave privada y del certificado asegura que ambas partes son quienes dicen ser y elimina cualquier riesgo de fraude, porque ni una ni otra podrán negar después que han participado en la operación, ni alterar los términos de la misma.

- **Despacho de Informes**

Bajo un proceso del tipo Batch: Deben existir controles que reduzcan las probabilidades de que un operario pueda robar información que sea confidencial, como las siguientes medidas:

-Log Accounting History, que son archivos que guardan historial. Indican día, hora, usuario y lo que hizo en el computador. El historial no puede ser borrado por el operador.

-Verificar el uso del papel de impresión, evitar el uso de papel autocopiativo.

-Verificar los folios de los documentos, y ver si falta alguno y por qué. El operador no puede destruir una impresión o un folio.

El despacho de informes es responsabilidad de informática mientras se encuentren en el área. También es responsabilidad de los usuarios verificar si los documentos que recibe están en las mismas condiciones en que fueron enviados.

Para procesos en línea: depende de cada persona, es cultural. Sólo hay seguridad de sistema operativo o por cláusulas de contrato en que se especifiquen multas o despidos por fuga de información.

El control de emisión de informes, puede apoyarse con TI, pero la parte fundamental está en las personas.

- **Respaldos**

Significa tener una copia a la cual se puede recurrir si la información principal se ha dañado o no pueda usarse. Existen:

-Respaldo de personas: es realizar capacitación a las personas para que puedan realizar reemplazos de otras personas que por ciertas circunstancias faltan. Esto se denomina Cross Posting. El respaldo de personas permite dar continuidad a los procesos.

-Respaldos de software y datos históricos: se guardan datos históricos y por lo general también los software que leen dichos datos. También se debe ir

adecuando los datos cada vez que se cambian los software. La periodicidad de los respaldos depende de la dinámica de actualización de lo que se desea respaldar, la cantidad de copias de respaldo depende de la importancia de lo que se respalda. El número mínimo de copias es 2 que deben estar separadas físicamente. A mayor cantidad de copias, mayor complejidad logística. Un respaldo que apoye funciones contables no puede ser destruido antes de cinco años, su eventual destrucción debe ser autorizada por las entidades regulatorias correspondientes (SII, etc.). Complementa a las técnicas de almacenamiento, como SAN, Mirroring, DSS, etc.

-Respaldos de software y datos de continuidad: apuntan a dar un servicio continuo, es decir, recuperar datos y/o software que un usuario haya perdido. La periodicidad es diaria y normalmente la cantidad de copias es 2. Normalmente se respalda diariamente los datos y/o software que ha sido modificado en el transcurso de tiempo que va desde el último respaldo efectuado, hasta el respaldo en proceso, una vez por semana se respalda todo. La decisión aquí es: Cuánto tiempo guardar el respaldo y va a depender de la importancia de la información y del costo de guardar los respaldos.

-Respaldos de hardware: en caso de que falle un servidor, se debe tratar de no afectar la continuidad, por lo que se puede reemplazar RAM, CPU, etc. Una opción es un disco nuevo y ocupar los respaldos de datos y software. Otra es colocar el disco de respaldo más actualizado si se tiene alguna copia, y aunque se recupere rápidamente la información, la del día se perderá. También se podría tener un servidor de respaldo.

Para los IVRS es necesario tener un respaldo, ya que estos equipos no pueden fallar. El equipo de respaldo tiene que permanecer siempre conectado aunque no esté en uso. En caso de falla, el coordinador desconecta ese equipo y utiliza el de respaldo hasta que el principal se repare.

-Respaldo de Discos Magnéticos: se tiene técnicas de almacenamiento como Hot repair, Mirroning, RAID, SAN.

-Equipos de comunicación y otros: se refieren códigos de barras, lector de tarjetas, etc. Lo ideal es tener otro equipo o sobredimensionar los equipos para darle continuidad al servicio.

-Respaldo de documentación: para los documentos, es necesario tener al menos una copia de la información, mientras más importante sea la información, mayor cantidad de copias.

1.4 Importancia de la seguridad

Ya definidos los tipos de seguridad, Para continuar es muy importante conocer el significado de dos palabras, que son riesgo y seguridad.

- **Riesgo**

Proximidad o posibilidad de un daño, peligro, etc.

Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

- **Seguridad**

Cualidad o estado de seguro

Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa.

Con estos conceptos claros podemos avanzar y hablar la criminología ya ha calificado los "delitos hechos mediante computadora "o por "sistemas de información" en el grupo de delitos de cuello blanco.

Crónica del crimen (o delitos en los sistemas de información)

- **Delitos accidentales e incidentales**

Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad.

En la actualidad los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras estos son:

-fraudes

-falsificación

-venta de información

Entre los hechos criminales más famosos en los E.E.U.U. están:

-El caso del Banco Wells Fargo donde se evidencio que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.

-El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.

-El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.

-También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

-También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una perdida de USD 3 millones.

Estos hechos y otros nos muestran claramente que los componentes del sistema de información no presentaban un adecuado nivel de seguridad. Ya que el delito se cometió con y sin intención. Donde se logró penetrar en el sistema de información.

Es por esto que ha surgido la necesidad por parte tanto de las empresas como de entes gubernamentales de reglamentar la seguridad y exigir medidas mínimas para estas.

En los últimos años, los gobiernos y los comités de estándares han exigido prestar una mayor atención a la privacidad de los clientes, a la confiabilidad de la información y a la seguridad. Por lo tanto, no sorprende que las corporaciones busquen optimizar su

política de cumplimiento y al mismo tiempo poder demostrar ese cumplimiento. Para esto se han dictado algunas normas y leyes como por ejemplo:

-La Ley Sarbanes-Oxley requiere que todas las compañías que cotizan en bolsa certifiquen que sus estados financieros y la información y los procedimientos utilizados para compilar los estados financieros sean anti-fraude.

-El sector de servicios financieros, entre otros, está sujeto actualmente a la Ley Gramm-Leach-Bliley y potencialmente al Acuerdo de Basilea II.

-Las corporaciones de los Estados Unidos deben proteger su información personal, y los proveedores de servicio médico y seguros deben proteger la información de sus pacientes a raíz de la Ley de Responsabilidad y Transferencia del Seguro Médico (HIPAA).

-La Ley Federal de Administración de la Seguridad de la Información (FISMA) requiere que las agencias federales desarrollen, documenten e implementen programas para proteger la información y los sistemas de información.

-Los programas utilitarios están sujetos a la norma de seguridad en el ciberespacio del Consejo de Confiabilidad Eléctrica de Norte América (NERC).

-En el extranjero, la Directiva de Protección de Datos de la Unión Europea requiere que todas las naciones miembro aprueben la legislación que exige controles de confidencialidad e integridad de las redes, los sistemas y los datos que contengan información personal. Mientras que gran parte de las reglamentaciones de los Estados Unidos se centran únicamente en la relación que tiene una organización con sus clientes externos, la Directiva de Protección de

Datos de la UE incluye explícitamente la información personal de los empleados además de la información de los clientes.

No sobra decir que el cumplimiento de la reglamentación es un desafío para las empresas actuales. Según una encuesta reciente de InformationWeek a 200 profesionales de tecnología empresarial, cuatro de cada cinco dijeron que es un desafío verificar si sus organizaciones logran las metas de cumplimiento de la reglamentación. Y cerca de dos tercios dijeron que el gasto en cumplimiento de la reglamentación será superior este año.

Es una situación abrumadora: las empresas, que trabajan con recursos limitados, afrontan cada vez más presión de los organismos reguladores – sin mencionar el desafío de hacer negocios en un entorno de amenazas en el ciberespacio cada vez peor. Entonces, ¿qué medidas pueden tomar para reducir las molestias que conlleva el cumplimiento? Veamos algunas de ellas.

- **Identificar y acceder a las políticas de administración** para definir los controles de acceso a los recursos y a las aplicaciones de TI.
- **Políticas de configuración** para definir cómo los recursos de TI se deben configurar para protegerlos.
- Una **infraestructura de seguridad de TI** para proteger una organización de los intrusos y ataques externos.
- **Procesos de control de vulnerabilidades** para descubrir y mitigar vulnerabilidades y errores en las políticas de seguridad.
- **Herramientas y procedimientos de monitoreo intenso** para detectar las amenazas internas y externas

Además, las compañías deben:

- Crear políticas de seguridad específicas que se centren en los comportamientos y procesos principales considerados más importantes con el fin de respaldar la estrategia y los objetivos empresariales.
- Documentar normas de seguridad básicas que protejan todos los componentes de la infraestructura de la información.
- Evaluar rigurosamente los sistemas de cumplimiento de las políticas y de las normas técnicas de seguridad y arreglar las discrepancias inmediatamente.
- Educar a los empleados sobre las razones para crear las políticas y normas puesto que los empleados son la clave del éxito.

Como una iniciativa comercial clave de las empresas actuales, el cumplimiento de la reglamentación genera más escrutinio que antes. Además hay mucho en juego: el incumplimiento puede ser costoso, lo que genera pérdida de clientes y de la confianza en las empresas, además de responsabilidad financiera y jurídica. Por esta razón, las empresas requieren un mecanismo que garantice la confidencialidad, integridad y disponibilidad de su información vital – es decir, un sistema pro-activo de seguridad de la información. Este sistema evita "ir tras" reglamentaciones al garantizar la implementación de personal, procesos y tecnología adecuados para centrarse en la evaluación de riesgos e instalación de sistemas de protección. En el entorno actual de crecientes amenazas, las empresas no pueden conformarse con menos.

1.4.1 Seguridad en Chile

El crecimiento explosivo del comercio electrónico en Chile y el mundo corona el cambio del orden mundial, producto del fenómeno de la globalización.

Pero aún falta resolver problemas en áreas como seguridad en la compra, disponibilidad y distribución de los productos.

Tan sólo tomando en cuenta el bombardeo publicitario de sitios de venta en Internet no es sorpresa que el comercio electrónico crece a velocidades exponenciales en todas partes del mundo. Lo que sí provoca desconcierto es la magnitud de sus cifras.

Un estudio de la empresa Forrester Research indica que para el año 2004 el comercio electrónico alcanzará los 6,9 billones de dólares a nivel mundial. De estos, la mitad corresponde a Estados Unidos. Luego Asia secunda la lista con un estimado de US$1,6 billones, seguida estrechamente por Europa con US$1,5.

Estados Unidos con su amplio desarrollo tecnológico es el líder en la materia, con la confluencia tanto de las transacciones entre empresas como con la compra minorista de miles de personas que desean obtener artículos a través de Internet.

En Asia como en Europa, en cambio, existe una preponderancia del comercio virtual entre empresas, marcando un desafío en esos continentes para acercar las ventajas del comercio electrónico al usuario común y corriente.

Para América Latina la compra virtual está todavía en pañales, ya que según el estudio de Forrester Research para el año 2004 la región alcanzaría recién los 82 mil millones de

dólares anuales, bastante menos que las cifras de sus otros pares. Esto porque Latinoamérica aún tiene un bajo desarrollo de Internet: un 2% a 3% de los 500 millones de latinoamericanos está conectado, cifra insignificante comparado con el más de 50% de los ciudadanos estadounidenses.

Pero en el último año Internet en América Latina se ha venido desarrollando de manera vertiginosa. Frente a este emergente mercado múltiples cadenas de Telecomunicaciones han tirado sus cables en la región para interconectarla, aumentando la oferta de servidores (proveedores de acceso a Internet) en un 300%. Además, el precio de los equipos computacionales, siempre caros, ha disminuido en el último tiempo, haciéndolo más conveniente para las clases medias y bajas.

No en vano la presencia de Internet en Brasil es la más grande en América Latina, seguida por la Argentina, otro importante usuario. Chile aspira como firme candidato en la lista, ya que el crecimiento de las tecnologías en nuestro país ha sido vertiginoso. En 1998 habían 200 mil usuarios de Internet en **Chile,** mientras que actualmente esa cifra llega a 1.200.000, alcanzando ya la estimación total que se preveía para este año.

Hoy en día, la forma de hacer negocios está cambiando, gracias a las nuevas tecnologías, y la masificación de la comunicación y la forma de intercambiar información. Éstas se han transformado en la clave de todo negocio exitoso y, ante esta coyuntura, se hace necesario para todo empresario, contar con una buena conexión a Internet y una red comunicacional de primera línea, ya que son éstas las que unen todos los sistemas de información.

Las redes comunicacionales son un conjunto de computadores conectados entre si, cuya función es facilitar la comunicación entre PCs a través de cables, fibra óptica u ondas electromagnéticas con la finalidad de compartir información (tanto hardware como software) desde un equipo a otro.

En las empresas, el activo más importante en el mundo moderno y globalizado que tenemos es justamente la información, pues sin ésta una empresa sencillamente no funciona.

En este sentido, la información es lo que le da vida a cualquier organización, cualquiera sea la naturaleza de ésta, y son las redes comunicacionales las vías por las cuales esta información fluye y permite a las personas comunicarse entre sí y utilizar recursos que no están físicamente en un determinado lugar. A su vez, estas redes a través de Internet están mucho más allá de la empresa. Están abiertas al mundo.

En este contexto, las redes comunicacionales son las que unen las organizaciones y al ser humano. Pensar en tener sistemas de información sin redes es inaudito; tanto es así, que si no existe una red, se acaba el trabajo, porque se corta la comunicación.

Las empresas se forman y funcionan a través de áreas, ya sea de producción, financiera o marketing, entre otras, y para lograr un mismo objetivo deben comunicarse para funcionar, y para esto existen las redes. Cualquier transacción, como por ejemplo una orden de compra, debe seguir un complejo proceso de comunicación a través de las redes de datos de forma tal que se consolidan los distintos sistemas de información, lo que es importante sobretodo, para la gestión, porque toda decisión se debe tomar con la mayor información posible, y muchas veces se hace en cuestión de segundos. Sin las redes comunicacionales esta información sería más lenta, ya que este sistema optimiza tiempo.

- **Seguridad de Redes**

La seguridad es un tema de alta prioridad para las empresas, y ese es el lado falible de las redes. En este momento el riesgo mayor son los ataques a la red, a través de virus o robos de información, y en este sentido las empresas también tienen riesgo de utilizar el sistema. Por ende, se debe invertir en seguridad de redes, a pesar que falta mucho por aprender en torno a este tema.

Uno de las formas de asegurar el PC, es la utilización de lo que se denomina cortafuegos, los que permiten ver la información de otros equipos autorizados conectados en red. Sin embargo, los ataques cada vez se hacen más sofisticados, por lo que los cortafuegos no garantizan seguridad absoluta. Por ende es necesario mantener permanentemente actualizados los sistemas, a través de los diversos parches que las empresas de software van creando, para evitar que aquellas vulnerabilidades que existan sean mal utilizadas.

Otra técnica de seguridad, es la creación de claves de acceso, y en este sentido, existe un sistema a través de claves que asegura la seguridad en la red, pero lo importante es crear una clave que sea difícil, pues muchas personas utilizan password fáciles de descifrar, como la fecha del cumpleaños, y por ende arriesgan del mismo modo la seguridad de sus PCs y de su entorno.

Siempre existen riesgos, pero es necesario utilizar este sistema para la comunicación, pues hay que correr riesgos a la hora de enfrentar el mundo actual, ya que hoy en día todo se traduce en comunicación e información.

- **La compra virtual**

Todo este auge de Internet ha promovido su uso para obtener productos y establecer transacciones comerciales. Sólo el último semestre del año pasado aparecieron sitios chilenos que se atrevieron a ofrecer productos en línea. Entre ellos destacan Falabella y Almacenes París, quienes profesionalizaron el servicio y lo hicieron conocido a través de publicidad en la televisión abierta.

Según un estudio de la Cámara de Comercio de Santiago (CCS) los montos transados por la compra virtual en 1999 en Chile fueron 2,6 millones de dólares y se cree que podría crecer sustancialmente a los US$25 millones este año. Por esto, las empresas reconocen cada vez más la importancia de estar presentes en esta nueva forma de hacer negocios.

Las ventajas del comercio electrónico radican en que los oferentes pueden rebajar sus costos – ya no existe un distribuidor intermediario, sino que el nexo es directo entre proveedor y comprador -, incrementar la productividad y expandir su mercado de gran forma, ya que a través de couriers y sistema de correos, se puede comprar artículos en otros países.

El usuario aprecia la comodidad y la rapidez de la compra virtual, pero además a través de él puede acceder a productos especiales que no se encuentran en el mercado local (sitios en el extranjero), sumado a las múltiples ofertas que las empresas hacen para fomentar el servicio.

Si existe algún punto negro en el tema de la compra virtual es la seguridad de los datos al momento de pagar con tarjeta de crédito, ya que la persona que cancela en esa modalidad debe llenar sus datos a través de la página Web.

Los piratas informáticos, o hackers, pueden acceder tanto a los sistemas desde donde

proviene o llega la información, o en aquellos por los cuales se transmite (en la red los datos generalmente deben pasar por varios computadores antes de llegar a su final destinación).

Como la compra virtual recién comienza en Chile, el problema de los hackers no es patente. Pero podría llegar a ser un problema si no se toman las medidas de seguridad necesarias. Por ejemplo, en marzo pasado dos jóvenes galeses de 18 años fueron detenidos por obtener los datos de 28 mil tarjetas de crédito de diferentes países como Estados Unidos, Inglaterra, Canadá, Tailandia y Japón, de las que gastaron U$3 millones. Debido a este tipo de robos los países desarrollados gastan grandes sumas de dinero en sistemas de seguridad, situación que sólo ahora se está dando en Chile.

Las grandes tiendas Chilenas como Falabella o Almacenes París usan el sistema Secure Socket Layer (SSL) que es catalogado por los expertos como uno de los más seguros. Este sistema utiliza un programa de encriptación que hace prácticamente ininteligible la información para cualquier extraño.

- **Las Tiendas Virtuales en Chile**

El número de tiendas virtuales en Chile ha aumentado considerablemente los últimos años. Según la Cámara de Comercio de Santiago, los rubros que más destacan son computación, música, libros y hogar, como menaje, electrónica y electrodomésticos.

En una investigación que realizó el diario El Mercurio adquiriendo diferentes productos, resultó que un 60% de las tiendas cumplieron con los plazos establecidos de entrega. Además, se detectaron problemas con el inventario disponible, ya que ofrecían productos en las páginas que finalmente no estaban en el stock "real" de la tienda.

Todas las señales hacen prever que el comercio electrónico está creciendo a grandes pasos. Además, se hacen estudios y se trabaja para poder superar las fallas del servicio.

En opinión del gerente de estudios de la Cámara de Comercio de Santiago, George Lever, "en seis meses a un año los servicios habrán mejorado, al igual que el servicio post-venta, la información y seguridad en los medios de pago. Un sitio rezagado en alguno de esos elementos va a perder mercado".

El gran problema se presenta en el tema de la seguridad ya que los clientes aun son reticentes a dar información por Internet y a comprar por este medio por la creencia de ser un medio “poco seguro”

Hoy en día no es necesario argumentar en defensa de la utilización de las llamadas Tecnologías de Información (TI), en beneficio de una gestión más productiva y costo-efectiva por parte de las empresas. Los conceptos de seguridad también han evolucionado en forma significativa, adaptándose a la nueva tecnología y formas de operación de los sistemas modernos. Así, han aparecido múltiples herramientas tecnológicas y metodologías que prometen solucionar el problema de la seguridad de la información de las organizaciones. Sin embargo, los avances en resultados concretos son en realidad, magros. Las expectativas no están siendo satisfechas y la gran mayoría de las organizaciones, tanto públicas como privadas, enfrentan serios problemas y pérdidas asociadas al indebido y/o insuficiente resguardo de la confidencialidad, integridad y disponibilidad de la información crítica para sus actividades. Revisemos los principales factores que inciden en la determinación de las medidas de seguridad para resguardar los activos de información de cualquier organización:

- Nivel de dependencia de las TI para el logro de la "misión": indudablemente, mientras mayor sea la dependencia de las TI, mayor será el grado de exposición a

los riesgos inherentes a la utilización de tecnologías, todavía altamente propensas a fallas que vulneran la seguridad.

- Sensibilidad al riesgo: las organizaciones pueden tener distinta sensibilidad al riesgo, la que depende fundamentalmente del impacto percibido ante la eventualidad de la materialización de alguna de las amenazas identificadas (o no).

- Imposiciones derivadas del contexto legal, contractual y/o reglamentario: algunas empresas están obligadas por ley, contrato o reglamentos de organizaciones a las que pertenezcan a cumplir con ciertas condiciones de seguridad. En estos casos no queda al criterio de la empresa y deberá implementar los controles establecidos.

.

Es por esto, la creciente necesidad de las organizaciones de crear sus propias políticas respecto a seguridad.

Capitulo II

Políticas de seguridad

2.1 Introducción

La política de seguridad es el conjunto de principios y reglas, propios de la organización, que declaran como se gestionará la protección de los recursos informáticos y activos de información.

El término **política de seguridad** se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de `términos generales', aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina **política de aplicación específica**.

Una política de seguridad ha de ser explícita y bien definida, identificando todos los sujetos y objetos en el sistema e incluir un conjunto de reglas que permitan determinar qué sujetos pueden acceder a qué objetos.

La política de seguridad es una declaración de intenciones de alto nivel que proporciona las bases para definir y delimitar responsabilidades. Deben ser los directivos, junto a especialistas informáticos, los que definan los requisitos de seguridad, identifiquen loa procesos prioritarios y decidiendo los recursos que deben gozar de una mayor protección.

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

está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto - las no contempladas - serían consideradas ilegales.

La política de seguridad debe contemplar aspectos como: nivel de dependencia de los SI, nivel de inversiones en SI, valor de los activos de información, amenazas, vulnerabilidad de los SI, costes de seguridad, estándares, procedimientos, fiabilidad y disponibilidad de los sistemas, aspectos legales, manejo de incidentes, auditorias, etc.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático.

- **Disponibilidad**

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

- **Utilidad**

  Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.

- **Integridad**

  La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

- **Autenticidad**

  El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- **Confidencialidad**

  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

- **Posesión**

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

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados **normativas** (aunque las definiciones concretas de cada documento que conforma la infraestructura de nuestra política de seguridad - política, normativa, estándar, procedimiento operativo...- es algo en lo que ni los propios expertos se ponen de acuerdo). La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos.

Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente en recomendaciones reemplazando la palabra "debe" con la palabra "debería".

Por otro lado las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos en detalle. Además las políticas deberían durar durante muchos años, mientras que las normas y procedimientos duran menos tiempo.

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos. Por ejemplo, una norma de seguridad de cifrado podría especificar el uso del estándar DES (Data Encryption Standard). Esta norma probablemente deberá será revisada o reemplazada en los próximos años.

Las políticas son distintas y de un nivel superior a los procedimientos, que son los pasos operacionales específicos que deben llevarse a cabo para lograr una cierta meta. Como ejemplo, hay procedimientos específicos para realizar copias de seguridad de la información contenida en los discos duros de los servidores.

Una declaración sobre políticas describe sólo la forma general de manejar un problema específico, pero no debe ser demasiado detallada o extensa, en cuyo caso se convertiría en un procedimiento.

Las políticas también son diferentes de las medidas de seguridad o de los mecanismos de control. Un ejemplo de esto último sería un sistema de cifrado para las comunicaciones o

para los datos confidenciales guardados en discos y cintas. En muchos casos las políticas definen metas u objetivos generales que luego se alcanzan por medio de medidas de seguridad.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles sobre cómo aplicar esta política. Por ejemplo, la metodología a usar para probar el software.

Un documento sobre políticas de seguridad contiene, entre muchos aspectos: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, manejo de virus e intrusos. También puede incluir la forma de comprobar el cumplimiento y las eventuales medidas disciplinarias.

2.2 Importancia de las Políticas

2.2.1 Asegurar la aplicación correcta de las medidas de seguridad

Con la ilusión de resolver los problemas de seguridad expeditamente, en muchas organizaciones simplemente se compran uno o más productos de seguridad. En estos casos, a menudo se piensa que nuevos productos (ya sea en hardware, software, o servicios), es todo que se necesita. Luego que se instalan los productos, sin embargo, se genera una gran desilusión al darse cuenta que los resultados esperados no se han materializado. En un número grande de casos, esta situación puede atribuirse al hecho que no se ha creado una infraestructura organizativa adecuada para la seguridad informática.

Un ejemplo puede ayudar a aclarar este punto esencial. Supóngase que una organización. También deben establecerse los procedimientos para que el personal técnicas implante el control de acceso de una manera cónsona con estas decisiones. Además debe definir la manera de revisar las bitácoras (logs) y otros registros generados por el sistema. Éstas y otros medidas constituyen parte de la infraestructura organizativa necesaria para que los productos y servicios de seguridad sean efectivos.

Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad. Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada, es decir, son los aspectos esenciales desde donde se derivan los demás.

2.2.2 Guiar el proceso de selección e implantación de los productos de seguridad

La mayoría de las organizaciones no tiene los recursos para diseñar e implantar medidas de control desde cero. Por tal razón a menudo escogen soluciones proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la organización. Esto se realiza a menudo sin conocer o entender suficientemente los objetivos y las metas de seguridad. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización.

Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere. De manera que tales políticas pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando los sistemas de seguridad.

2.2.3 Demostrar el apoyo de la Presidencia y de la Junta Directiva

La mayoría de las personas no está consciente de la gravedad de los riesgos relativos a la seguridad y por eso no se toma el tiempo para analizar estos riesgos a fondo. Además, como no tiene la experticia suficiente, no es capaz de evaluar la necesidad de ciertas medidas de seguridad. Las políticas son una manera clara y definitiva para que la alta gerencia pueda mostrar que:

1. La seguridad de los activos de información es importante

2. El personal debe prestar la atención debida a la seguridad.

Las políticas pueden entonces propiciar las condiciones para proteger los activos de información. Un ejemplo muy frecuente involucra a los gerentes a nivel medio que se resisten a asignar dinero para la seguridad en sus presupuestos. Pero si las políticas que han sido emitidas por la Junta Directiva o la alta gerencia, entonces los gerentes a nivel medio no podrán continuar ignorando las medidas de seguridad.

2.2.4 Evitar responsabilidades legales

Se presentan cada vez más casos judiciales en los cuales se encuentra responsables a empleados, y particularmente a gerentes, de no actuar apropiadamente bien en lo referente a seguridad informática. La razón puede ser atribuida a: negligencia, violación

de confianza, fallas en el uso de medidas de seguridad, mal práctica, etc. Estos casos se usan a menudo con éxito para llamar la atención de la gerencia y para lograr apoyo para los esfuerzos en seguridad informática.

2.2.5 Lograr una mejor seguridad

Uno de los problemas más importantes en el campo de seguridad informática lo representan los esfuerzos fragmentados e incoherentes. A menudo un departamento estará a favor de las medidas de seguridad, mientras que otro dentro de la misma organización se opondrá o será indiferente. Si ambos departamentos comparten recursos informáticos (por ejemplo una LAN o un servidor), el departamento que se opone pondrá en riesgo la seguridad del otro departamento y de la organización completa. Aunque no es ni factible ni deseable que todas las personas en una organización se familiaricen con las complejidades de la seguridad informática, es importante que todas ellas se comprometan con mantener algún nivel mínimo de protección. Las políticas pueden usarse para definir el nivel de esta protección mínima, a veces llamada línea de base.

Pueden coexistir, en una misma organización, diferentes políticas no contradictorias en sus diferentes niveles o incluso en el mismo nivel.

2.3 Tipos de políticas

Las políticas se clasifican en tres grupos: administrativas, de control de acceso y de flujo de administración.

- Las políticas administrativas emplean procedimientos administrativos, no técnicos.

- Las políticas de control de acceso establecen las condiciones en que un sujeto, particularmente un programa, puede acceder a un objeto.

- Las políticas de control de flujo tratan de la difusión de la información, estableciendo los canales legítimos para ello.

2.3.1 Políticas administrativas

En este grupo se incluyen las políticas que se establecen a la hora del desarrollo de aplicaciones.

Ejemplos típicos son la modularización de las aplicaciones, las pruebas cruzadas, la revisión de los módulos por programadores diferentes, etc.

2.3.2 Políticas de control de acceso

Existen diferentes políticas para condicionar el acceso a los objetos (entidades pasivas que contienen o reciben información) por parte de los sujetos (personas o programas).

Ejemplos de objetos son: dispositivos de almacenamiento, páginas de memoria, tablas del sistema operativo, estructuras de datos, ficheros, directorios de ficheros, etc.

Se denomina granularidad al tamaño mínimo de los objetos a los que se puede acceder. La granularidad varía enormemente desde la más gruesa (p.e. un disco completo) a la más fina (p.e. sólo un campo de un registro). La seguridad disminuye al aumentar la granularidad.

- La **política de menor privilegio**, o "de necesidad de saber", establece que los usuarios sólo acceden a los objetos necesarios para su trabajo.

- La **política de compartición**, o de máximo privilegio, permite el acceso de todos los sujetos a todos los objetos. Normalmente sólo se usan en departamentos de investigación y en trabajos en grupo.

- La **política abierta** autoriza todo acceso, salvo que esté explícitamente denegado.

- La **política cerrada** prohíbe cualquier acceso, salvo que esté explícitamente permitido. Es más segura que la abierta, pero sobrecarga fuertemente el sistema.

Todas estas políticas no se preocupan de como, una vez obtenido el acceso al dato, el programa utiliza la información. Podría. por ejemplo, ser transmitida a través de los llamados canales ocultos o canales ilícitos, a usuarios no autorizados.

2.3.3 Políticas de control de flujo

En estas políticas es necesario priorizar las tres características de la información (confidencialidad o secreto, integridad o no modificación y disponibilidad o la no destrucción).

El orden de prioridad depende del tipo de organismo. Así los organismos de defensa y seguridad anteponen la confidencialidad a la disponibilidad y esta a la integridad. Los económicos priorizan la integridad, siguiendo la disponibilidad y la confidencialidad. Las instituciones gubernamentales no incluidas en el primer grupo eligen primero la integridad, después la confidencialidad y por último la disponibilidad.

Las políticas de control de flujo se dividen en **políticas discrecionales** y **políticas obligatorias** (o no discrecionales). Ambas pueden coexistir en una misma empresa, aunque en diferentes niveles.

En las políticas discrecionales el propietario de un objeto concede o no discrecionalmente el acceso a otros sujetos.

En las políticas obligatorias se establece se establece un conjunto de compartimentos de objetos y sujetos y una clasificación de ambos en niveles de confidencialidad. Un sujeto sólo puede acceder a un objeto si ambos pertenecen al mismo compartimento y además el nivel de confidencialidad de aquel es igual o mayor que el del objeto.

2.4 Políticas de Seguridad Informática

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Esto ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

2.4.1 Definición

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada PSI es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

2.4.2 Elementos

Como hablamos en la sección anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

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

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

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

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

2.5 Metodología para el Desarrollo de Políticas y Procedimientos en Seguridad de Información

Antes de embarcarse en un esfuerzo de elaborar las políticas de seguridad, es aconsejable aclarar quién es responsable de promulgarlas y aplicarlas. Solamente cuando exista claramente la asignación clara de responsabilidades. Si se ignora este paso importante, se corre el riesgo de posteriores objeciones, críticas y malentendidos, que pueden significar problemas y grandes retrasos.

Otro requisito previo necesario para tener éxito involucra la perspectiva de la Junta Directiva y la alta gerencia. Sólo después de que sus miembros tomen conciencia de que los activos de información son un factor vital para el éxito de la organización, es que la seguridad informática es apreciada como un asunto serio que merece atención. En caso contrario probablemente no apoyen la idea de establecer políticas de seguridad

La alta gerencia debe darse cuenta que hay problemas serios de seguridad y que se requiere de políticas para afrontarlos. Si bien esto puede parecer obvio, muchos intentos de desarrollar e implantar las políticas no ha llegado a ninguna parte porque no se habían echado las bases. El trabajo previo incluye a menudo una breve presentación a la alta gerencia para sensibilizarla sobre la necesidad de la seguridad informática.

Idealmente, el desarrollo de políticas de seguridad debe comenzarse después de una evaluación a fondo de las vulnerabilidades, amenazas y riesgos. Esta evaluación debería

indicar, quizás sólo a grandes rasgos, el valor de la información en cuestión, los riesgos a los cuales esa información se sujeta, y las vulnerabilidades asociadas a la manera actual de manejar la información. También pueden ser incluidos en la declaración de las políticas, los tipos generales de riesgos enfrentados por la organización, así como cualquier otra información útil obtenida a partir del análisis de riesgos.

Un buen momento para desarrollar un conjunto de políticas de seguridad es cuando se está preparando el manual de seguridad para los activos de información. Debido a que ese manual va a ser distribuido a lo largo de toda la organización, representa un medio excelente para incluir también las políticas de seguridad. También pueden publicitarse las políticas en material tal como video, carteles o artículos en un periódico interno.

Otro bueno momento es después de que haya ocurrido una falla grave en seguridad, por ejemplo una intrusión de hackers, un fraude informático, un accidente sin poder recuperar los datos, un incendio y en general algún tipo de daño o perjuicio que haya recibido la atención de la alta gerencia. En este caso habrá un alto interés en que se apliquen las políticas de seguridad y que se implanten medidas más efectivas. Hay que actuar rápidamente para desarrollar las políticas, ya que el nivel de preocupación de los gerentes y de los empleados tiende a decrecer luego que ha pasado el incidente.

Un buen objetivo a tener presente cuando se redactan las políticas, es que ellas deberían durante varios años, por ejemplo cinco años. En realidad, se harán modificaciones más a menudo, pero para evitar que se vuelvan obsoletas rápidamente, debe elaborarse para que sean independientes de productos comerciales específicos, estructuras organizativas específicas, así como las leyes específicas y regulaciones.

Las cosas mueven muy rápidamente en el campo de tecnología, incluyendo la seguridad informática. Por ejemplo, hace apenas algunos años la mayoría de las organizaciones no

creían que era necesaria una política de seguridad para Internet, pero hoy día es muy importante.

Las políticas deben revisarse en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables. Este esfuerzo también ayudará a mejorar la credibilidad de las actividades de seguridad informática dentro de la organización. Los empleados apreciarán que el personal de seguridad informática no está allí para crear más burocracia, sino para realmente ocuparse de las medidas de seguridad requeridas para proteger los recursos.

2.5.1 Elaboración de las Políticas

2.5.1.1 Recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.

Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

2.5.1.2 Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir

políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

2.5.1.3 Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos redactar las políticas, para lo cual pueden servir de ayuda el ejemplo que se encuentra más adelante.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporciona mucho más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Este comité debería tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar las políticas en la luz de su viabilidad, análisis costo/beneficio y sus implicaciones. Las preguntas que debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables?. ¿Son estas políticas claras e inequívocas?

Es muy importante que la Junta Directiva apruebe las políticas en el caso frecuente que ciertos empleados objeten o piensen que ellos no necesitan obedecer.

Además es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

La aplicación de nuevas políticas es a menudo más eficaz si los empleados han sido informados de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.

Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Allí, por ejemplo, se explicaría que la información interna es la propiedad de organización, y que no puede ser copiada, modificada, anulada o usada para otros propósitos sin la aprobación de la gerencia.

- **La longitud del documento sobre las políticas**

Las políticas de seguridad deben diseñarse de acuerdo a las necesidades específicas e una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas. Como ejemplo, el manual sobre las políticas de seguridad de British Telecom (una compañía telefónica británica) es de más de 150 páginas, mientras que el de Lockheed (una compañía aerospacial) es de 75 páginas.

El personal de seguridad puede opinar que es necesario que todo esté absolutamente claro y explícito sobre los asuntos de seguridad informática. En estos casos puede que se requiere un conjunto de políticas. Otros serán renuentes a tener tantas políticas, prefiriendo enfatizar la confianza en buen juicio y buen comportamiento de los empleados.

Aunque un documento conciso será leído y asimilado con más probabilidad, hay mucho a favor de un conjunto completo y extenso de políticas de seguridad. Un principio

general es que se deben promulgar sólo aquellas políticas que sean absolutamente necesarias. Esto es debido a que las personas son inherentemente muy diferentes entre sí, como también son diferentes los grupos a que pertenecen. El imponer un único conjunto de reglas para todos puede llevar a resistencia y a pobres resultados. En cambio, al tener sólo aquellas políticas que son estrictamente necesarias, se favorece la iniciativa personal y la creatividad. Además tantas políticas de seguridad van a impedir que el trabajo se haga a tiempo.

En todo caso, en vez de emprender un trabajo a fondo, es mejor empezar primero ocupándose de los aspectos esenciales, para luego ir ampliando con políticas adicionales. Este procedimiento toma a menudo la forma de declaraciones separadas que se tratan las áreas problemáticas, por ejemplo PCs, LANs e Internet. De esta manera es también más fácil conseguir la aprobación de la alta gerencia así como de los propios empleados. Por otro lado las políticas nunca pueden tomar en cuenta todas las circunstancias y un conjunto extenso y minucioso de políticas puede generar críticas, disgusto y rechazo.

La extensión y el grado de detalle de las políticas es una función de tipo de audiencia y puede haber distintos documentos según el caso. Por ejemplo, podría haber documentos para los usuarios, la gerencia y el personal de informática. Muchas de las políticas en cada uno de estos documentos serían iguales, aunque el grado de detalle, las palabras técnicas utilizadas, y el número de ejemplos puede variar de un documento a otro. Para los usuarios finales, el documento debe limitarse a unas cuantas páginas. Para la gerencia habrá consideraciones adicionales, tal como los aspectos legales, y es probable que esto extienda el documento. Para el personal técnico será todavía más largo y más detallado.

Otro factor que afecta es el grado de seguridad requerido en la organización. En general, cuánto mayor es el uso de la información para las actividades de una organización, mayor es la necesidad de seguridad. Por ejemplo, un banco tendrá muchas y extensas

políticas, mientras que una cadena de tiendas por departamentos tendrá menos políticas. Por supuesto que actividades especialmente delicadas, tal como salud y defensa, requieren de políticas muy detalladas.

Adicionalmente al número de políticas, hay que plantearse cuán larga debe ser la definición de cada política. Las definiciones concisas, de unas cuantas frases, son más aceptadas por los empleados ya que son más fácilmente leídas y entendidas. En todo caso deben ser suficientemente específicas para ser entendidas e interpretadas sin ambigüedad, pero no deben ser tan específicas que impidan adaptarlas a las condiciones particulares de un sitio o departamento. Por ejemplo, se puede promulgar una política la cual especifica que todos los usuarios deben usar contraseñas difíciles de adivinar. Esta política da la flexibilidad a un gerente local para determinar su longitud mínima o un sistema automático que chequee si realmente una dada contraseña es difícil de adivinar.

Para ayudar a aclarar qué son las políticas, se pueden incluir ejemplos específicos. Como ilustración, una política que prohíbe el uso de los recursos computacionales para fines personales podría incluir ejemplos sobre Internet Chat Relay (IRC) o juegos por computadora.

Si se opta por elaborar un conjunto muy completo de políticas de seguridad, se aconseja hacerlo en dos etapas. El primer paso involucra el obtener la aprobación de la Junta Directiva para un conjunto genérico de políticas, mientras que el segundo paso involucra la aprobación para un conjunto más específico de políticas. El conjunto genérico podría incluir de 10 a 20 políticas, y el juego específico podría incluir otras 50-100.

De hecho, si el conjunto inicial de políticas es demasiado largo o severo, la Junta Directiva puede rechazarlo. Como resultado, la ventana de tempo para conseguir la aprobación puede cerrarse por un cierto periodo de tiempo (a menudo un año o más). Así que se aconseja elaborar un primero conjunto de políticas corto y relativamente fácil

de cumplir por parte del personal. Después, cuando haya sido implantado y asimilado a lo largo de la organización, se puede preparar una lista más completa y más estricta. Es mucho mejor proceder de forma relativamente lenta, con una serie pasos en el desarrollo de políticas, y así lograr credibilidad y apoyo, que preparar de una vez un solo documento extenso con todas las políticas, el cual se rechaza porque fue percibido como engorroso o excesivamente severo.

2.6 Modelos de Seguridad

El principal inconveniente de las políticas de seguridad es que están expresadas en lenguaje natural, lo cual siempre conlleva ambigüedades de interpretación. Por ello se han desarrollado los Modelos de Seguridad como formulaciones teóricas, expresables matemáticamente, de las políticas de seguridad.

Un modelo de seguridad debe contener los elementos suficientes para que los diseñadores del sistema conozcan lo necesario para determinar los controles de seguridad a construir, para que los usuarios puedan utilizar eficazmente el sistema, y para que los evaluadores puedan determinar su consistencia y adecuación a las políticas y su correcta implantación.

En los modelos de seguridad es necesario definir restricciones que eviten la ejecución de programas que puedan afectar a la seguridad del sistema. Las restricciones, en forma de axiomas, controlan el tipo de acceso a un objeto permitido a un sujeto, constituyendo un filtro obligatorio para todo intento de acceso.

2.6.1 Tipos de modelos

Existen dos grupos de modelos de seguridad: **modelos de seguridad discrecional y modelos de seguridad obligatoria.**

Los modelos discrecionales se basan en las políticas discrecionales y se expresan mediante los modelos de matriz de acceso y el modelo de Take-Grant.

Los modelos obligatorios especifican los canales lícitos por los que pueden circular la información. Se dividen en modelos multinivel y modelos de flujo de información.

2.6.2 Parámetros para establecer políticas de seguridad

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

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

- Involucre a los áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas

- Un consejo más, no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

2.6.3 Motivos por los cuales no se logra implementar las políticas.

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una travesura puede convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las PSI logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridades necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación, algunas recomendaciones para "vender" las preocupaciones sobre la seguridad informática:

- Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asocie el punto anterior a las estrategias de negocio y la imagen de la empresa en el desarrollo de sus actividades.
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.
- Muestre una valoración costo-beneficio, ante una falla de seguridad.
- Desarrolle las justificaciones de la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización

- Un consejo más, sea oportuno y sagaz para presentar su producto, procurando tener la mayor información del negocio y los riesgos asociados con los activos críticos de la organización.

2.6.4 Las políticas de seguridad informática como base de la Administración de la seguridad integral.

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

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

2.7 Ejemplo de Políticas de Seguridad

2.7.1Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas gerencias de la Compañía están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva que muestre el estado actual de la Compañía en cuanto a seguridad informática y los progresos que se han logrado.

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

2.7.2Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Compañía:

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

- La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo

largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

- Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

    - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

- No divulgar información confidencial de la Compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

2.7.3 Políticas de Seguridad para computadores

- Los computadores de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática
- No se permite fumar, comer o beber mientras se está usando un PC.

- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

- Si un PCs tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Compañía.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales..

- Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.

- No pueden extraerse datos fuera de la sede de la Compañía sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.

- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Compañía debe guardarse en otra sede, lejos del edificio.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.

- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

- Siempre que sea posible, deba eliminarse información confidencial de de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto

no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Compañía.

- No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañía.

- El personal que utiliza un computador portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

2.7.4. Políticas de seguridad para las comunicaciones

2.7.4.1 Propiedad de la información:

Con el fin de mejorar la productividad, la Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no propiedad de los usuarios de los servicios de comunicación.

2.7.4.2 Uso de los sistemas de comunicación

- Los sistemas de comunicación de la Compañía generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además

no interfiera con la productividad del empleado ni con las actividades de la Compañía.

- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

2.7.4.3 Confidencialidad y privacidad

- Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outolook, Outlook Express u otros productos previamente aprobados por la Gerencia de Informática.

- Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

- Es política de la Compañía no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser

supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

- De manera consistente con prácticas generalmente aceptadas, la Compañía procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

2.7.4.4 Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

2.7.4.5 Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

2.7.5 Políticas de seguridad para redes

2.7.5.1 Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras.

2.7.5.2 Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

2.7.5.3 Aspectos generales

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

2.7.5.4 Modificaciones

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la Compañía, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

2.7.5.5 Cuentas de los usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

- No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

- Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los

privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

2.7.5.6 Contraseñas y el control de acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña,

luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

- Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.

- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

- Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y

las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

Capitulo III

Estándares

3.1 Introducción

Como hemos visto en los anteriores capítulos, la seguridad de información con TI es un tema muy amplio, ya que abarca todos los ámbitos de las empresas, y todo tipo de negocios, es por ello que se hace muy necesaria la elaboración de estándares para manejar la seguridad.

Estos estándares se pueden clasificar en:

- **Estándares para la administración de la seguridad de la información**
- **Estándares para evaluación de seguridad en sistemas**
- **Estándares para el desarrollo de aplicaciones**
- **Estándares para riesgo**
- **Etc.**

Esto dependerá de la orientación o alcance del estándar.

Por lo que podemos ver existe una gran variedad de estándares que podemos aplicar, sin dejar de mencionar que además las empresas u organizaciones pueden crear sus propios estándares, según sus necesidades.

Pero hoy en día donde los mercados no son cerrados, sino más bien abiertos por la globalización, es necesario, sino indispensable cumplir con normas internacionales, y certificarse internacionalmente, es por esto que la existencia de estándares para estos fines se hace indispensable para las empresas actualmente.

A continuación se elabora una lista de estándares internacionales de seguridad en sistemas de información y se dará una reseña de su contenido y objetivo. Para un mejor entendimiento se han separado lo que es **Instituciones de normalización y normas de evaluación y certificación**.

3.2 Instituciones de Normalización

Internacionales

3.2.1 ITU-T

La sigla ITU-T o UIT, corresponden a "**Unión Internacional de Telecomunicaciones**".

Cada vez que alguien, en cualquier parte, toma el teléfono y marca un número, responde a una llamada con un móvil, envía un fax o recibe un mensaje electrónico, toma un avión o un barco, escucha la radio, mira su programa de televisión favorito o ayuda a un niño a manejar el último juguete con control remoto, está beneficiándose de la labor de la Unión Internacional de Telecomunicaciones.

La Unión, que fue creada el siglo pasado, es una organización imparcial e internacional en la cual los gobiernos y el sector privado pueden trabajar juntos para coordinar la explotación de redes y servicios de telecomunicaciones y promover el desarrollo de la tecnología de comunicaciones. A pesar de seguir siendo relativamente desconocida para el gran público, la labor que viene desarrollando desde hace más de 100 años ha ayudado a crear una red mundial de comunicaciones que integra hoy una gran variedad de tecnologías y que sigue siendo uno de los sistemas más fiables que el hombre haya realizado jamás.

A medida que se amplía la utilización de las tecnologías de telecomunicaciones y de los sistemas de radiocomunicaciones para abarcar más y más actividades, la labor que realiza la ITU crece en importancia en la vida cotidiana de los habitantes de todo el mundo.

Las actividades de normalización de la Unión, que ya han ayudado a promover la expansión de nuevas tecnologías como la telefonía móvil e Internet, están sirviendo ahora para definir las bases sobre las cuales se construye la incipiente infraestructura mundial de la información y para el diseño de sistemas multimedios avanzados capaces de procesar fácilmente señales de voz, datos, audio y vídeo.

Al mismo tiempo, la ITU sigue realizando su labor de gestión del espectro de frecuencias radioeléctricas, gracias a la cual los sistemas de radiocomunicaciones, como los teléfonos celulares y los aparatos de radiobúsqueda, los sistemas aéreos y de navegación marítima, las estaciones de investigación espacial, los sistemas de comunicaciones por satélite y los de radiodifusión sonora y de televisión continúan funcionando sin interrupción y proporcionan servicios inalámbricos fiables a los habitantes del planeta.

Por último, es cada vez más importante el papel catalizador de la ITU en el proceso de formación de asociaciones para el desarrollo entre gobiernos y sector privado, gracias al cual la infraestructura de telecomunicaciones de las economías en desarrollo está mejorando rápidamente.

Tanto en lo que respecta al desarrollo de las telecomunicaciones como a la elaboración de normas o a la compartición del espectro, la filosofía de consenso de la ITUayuda a los gobiernos y a la industria de las telecomunicaciones a afrontar y a tratar una gran cantidad de asuntos que serían difíciles de resolver a nivel bilateral.

El resultado de ello son acuerdos reales y viables que no sólo benefician al sector de las telecomunicaciones en su totalidad, sino también, y en última instancia, a los usuarios de telecomunicaciones de todo el mundo.

Los fines de la Unión Internacional de Telecomunicaciones, tal como están definidos en su Constitución, son los siguientes:

- mantener y ampliar la cooperación internacional entre todos sus Estados Miembros para el mejoramiento y el empleo racional de toda clase de telecomunicaciones
- alentar y mejorar la participación de entidades y organizaciones en las actividades de la Unión y favorecer la cooperación fructífera y la asociación entre ellas y los Estados Miembros para la consecución de los fines de la Unión
- promover y proporcionar asistencia técnica a los países en desarrollo en el campo de las telecomunicaciones y promover asimismo la movilización de los recursos materiales, humanos y financieros necesarios para dicha asistencia, así como el acceso a la información de estos países
- impulsar el desarrollo de los medios técnicos y su más eficaz explotación, a fin de aumentar el rendimiento de los servicios de telecomunicación, acrecentar su empleo y generalizar lo más posible su utilización por el público
- promover la extensión de los beneficios de las nuevas tecnologías de telecomunicaciones a todos los habitantes del planeta
- promover la utilización de los servicios de telecomunicaciones con el fin de facilitar las relaciones pacíficas

- armonizar los esfuerzos de los Estados Miembros y favorecer una cooperación y una asociación fructíferas y constructivas entre los Estados Miembros y los Miembros de los Sectores para la consecución de estos fines

- promover a nivel internacional la adopción de un enfoque más amplio de las cuestiones de las telecomunicaciones, a causa de la globalización de la economía y la sociedad de la información, cooperando a tal fin con otras organizaciones intergubernamentales mundiales y regionales y con las organizaciones no gubernamentales interesadas en las telecomunicaciones.

3.2.1.1 Funciones y actividades

La Unión Internacional de Telecomunicaciones se diferencia de todas las demás organizaciones internacionales en que se basa en el principio de la cooperación entre gobiernos y sector privado. Sus Miembros son instituciones políticas y de reglamentación en telecomunicaciones, operadores de redes, fabricantes de equipo, realizadores de equipos y programas informáticos, organizaciones regionales de normalización e instituciones de financiación, por lo cual puede afirmarse que las actividades, las políticas y la dirección estratégica de la ITU están determinadas y concebidas por el sector al que sirve.

Funciones en plena evolución

El clima en el que la ITU desarrolla su labor en la actualidad es muy diferente del que existía 135 años atrás cuando la organización fue fundada. En los últimos 20 años, las telecomunicaciones han pasado de ser un instrumento que facilitaba las comunicaciones de individuo a individuo a convertirse en la base sobre la que se realizan un gran número de actividades que van desde el comercio internacional a la atención sanitaria y, cada vez más, la educación. Hoy son vitales las redes de telecomunicaciones rápidas y fiables

para la provisión a través de las fronteras de servicios como la banca, el transporte, el turismo, la información en línea y la compra electrónica desde el hogar.

Al mismo tiempo, los individuos e instituciones a los que sirve la Unión también están cambiando, debido a que la forma de prestar servicios de telecomunicaciones ha evolucionado, y también a la convergencia de los sectores de las comunicaciones, la informática y el entretenimiento audiovisual. La liberalización y la desregularización del sector de las telecomunicaciones en muchos países han hecho que los Miembros tradicionales de la ITU pidan a la organización que les proporcione nuevos servicios, sobre todo en relación con el desarrollo de políticas y la orientación en materia de reglamentación.

Además, un número cada vez mayor de organizaciones dedicadas a actividades como el desarrollo de programas informáticos, el entretenimiento y la radiodifusión, comienza a interesarse en formar parte de la ITU, ya que sus actividades se orientan cada vez más hacia servicios basados en las telecomunicaciones.

En este entorno en plena evolución, la ITU también se está transformando para conservar su relevancia, seguir respondiendo a las nuevas necesidades de sus Miembros más antiguos y poder reconocer y colmar las expectativas de los más recientes.

3.2.1.2 Estructura y actividades

Los tres Sectores de la Unión, Radiocomunicaciones (ITU-R), Normalización de las Telecomunicaciones (ITU-T) y Desarrollo de las Telecomunicaciones (ITU-D), trabajan en la actualidad para construir y configurar las redes y servicios del mañana. Sus actividades cubren todos los aspectos de las telecomunicaciones, desde el establecimiento de normas que faciliten el interfuncionamiento sin interrupciones de equipos y sistemas a nivel mundial, hasta la adopción de procedimientos operativos para la vasta y creciente gama de servicios inalámbricos, pasando por la concepción de

programas para mejorar la infraestructura de telecomunicaciones en el mundo en desarrollo. Gracias a la labor de la UIT se han sentado las bases fundamentales que han permitido que el sector mundial de las telecomunicaciones ascienda hoy a un valor de 1billón USD.

La labor de cada uno de los Sectores de la ITU se desarrolla en conferencias y reuniones en las que los Miembros negocian los acuerdos que servirán de base para la explotación de servicios mundiales de telecomunicaciones.

El trabajo técnico de la Unión, que consiste en la preparación de estudios exhaustivos sobre la base de los cuales se formulan Recomendaciones muy bien aceptadas, corre a cargo de comisiones de estudio constituidas por expertos procedentes de organizaciones de telecomunicaciones líderes de todo el mundo.

El ITU-R determina las características técnicas de los servicios y sistemas inalámbricos terrenales y espaciales, y desarrolla procedimientos operativos. Asimismo, realiza importantes estudios técnicos que sirven como base para las decisiones en materia de reglamentación que se toman en las conferencias de radiocomunicaciones.

En el ITU-T, los expertos preparan especificaciones técnicas sobre el funcionamiento, el rendimiento y el mantenimiento de los sistemas, redes y servicios de telecomunicaciones. Estos expertos se encargan también de los principios de tarificación y de los métodos de contabilidad que se utilizan en la prestación de servicios internacionales.

La labor fundamental de los expertos del ITU-D es preparar recomendaciones, opiniones, directrices, manuales, libros de referencia e informes en los que se ofrece a los altos ejecutivos de los países en desarrollo información sobre «las prácticas más recomendables» en ámbitos que van desde las estrategias y políticas de desarrollo a la gestión de las redes.

Actualmente la Unión cuenta con 22 comisiones de estudio repartidas entre sus tres Sectores (7en el UIT-R, 13 en el UIT-T y 2 en el UIT-D), que en total elaboran unas 550 Recomendaciones nuevas o revisadas cada año. Las Recomendaciones de la ITU son acuerdos de carácter facultativo, no vinculantes.

Cada Sector tiene también su propia oficina encargada de la ejecución de su plan de trabajo y de la coordinación de las actividades a nivel cotidiano

Los Miembros de la ITU

La ITU está abierta a todos los Estados, que pueden convertirse en Estados Miembros de la Unión, así como a organizaciones privadas como los operadores, fabricantes de equipo, organismos de financiación, organizaciones de investigación y desarrollo y organizaciones internacionales y regionales de telecomunicaciones, que pueden hacerse Miembros de uno de los Sectores de la ITU.

Dado que las telecomunicaciones son un factor cada vez más importante para el crecimiento de la actividad económica mundial, pertenecer a la ITU ofrece a los gobiernos y a los organismos privados la oportunidad de participar activamente en una organización que cuenta con más de 130 años de experiencia en la construcción de las redes de comunicaciones del mundo.

Al ser Miembros de la organización de telecomunicaciones más importante, más respetada y más influyente del mundo, los Estados y las empresas privadas pueden hace oír su voz y realizar una importante y valiosa contribución a los avances que están cambiando nuestro mundo.

La participación directa en la labor de la ITU proporciona a todos sus Miembros la oportunidad de influir, participar y adquirir experiencia en el proceso de construcción de un nuevo mundo para un nuevo milenio.

Las empresas privadas y otras organizaciones pueden formar parte de uno o varios de los tres Sectores de la Unión, de acuerdo con sus intereses específicos. Ya sea a través de su participación en conferencias, asambleas y reuniones de carácter técnico o en la labor del día a día, los Miembros se benefician de una oportunidad única de establecer contactos y de un foro de encuentro universal en el que pueden examinar diversos asuntos, entablar negociaciones y establecer asociaciones. Los Miembros de Sector de la ITU participan también en la elaboración de las normas técnicas en las que se basarán los futuros sistemas de telecomunicaciones y las redes y servicios del mañana.

Por último, los Miembros de Sector tienen acceso privilegiado a información restringida de primera mano que puede resultarles muy valiosa en su planificación empresarial.

Dada su función singular y su larga historia en el ámbito de las telecomunicaciones mundiales, la ITU constituye el foro ideal para que los gobiernos y el sector privado se reúnan y establezcan programas y marcos políticos que tendrán una extraordinaria influencia en el futuro de la industria mundial.

El principal objeto de la presente Lista es enumerar todas las Recomendaciones ITU-T (antiguo CCITT) que se hallan en vigor en la fecha de publicación de esta Lista. Además, los Suplementos del CCITT/UIT-T que contienen información relativa a la explotación u otros tipos de informaciones prácticas o relacionadas con la realización en el ámbito de una determinada Serie de Recomendaciones se enumeran al final de dicha Serie en esta Lista.

3.2.1.3 Lista de Recomendaciones ITU-T en vigor

- **SERIE A**

Organización del trabajo del ITU-T: se refiere a como debe trabajar y orientar el trabajo la institución, en cuanto a métodos, grupos temáticos, proceso de aprobación de las recomendaciones. Etc.

- **SERIE B**

Medios de expresión: definiciones, símbolos, clasificación: Adopción del lenguaje de especificación y descripción (LED) del CCITT

- **SERIE C**

Estadísticas generales de telecomunicaciones: esta serie fue suprimida.

- **SERIE D**

Principios generales de tarificación

- **SERIE E**

Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos

- **SERIE F**

Servicios de telecomunicación no telefónicos

- **SERIE G**

Sistemas y medios de transmisión, sistemas y redes digitales

- **SERIE H**

Sistemas audiovisuales y multimedios

- **SERIE I**

Red digital de servicios integrados

- **SERIE J**

Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios.

- **SERIE K**

Protección contra las interferencias

- **SERIE L**

Construcción, instalación y protección de los cables y otros elementos de planta exterior

- **SERIE M**

RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímile y circuitos arrendados internacionales

- **SERIE N**

Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión

- **SERIE O**

Especificaciones de los aparatos de medida

- **SERIE P**

Calidad de transmisión telefónica, instalaciones telefónicas y redes locales

- **SERIE Q**

Conmutación y señalización

- **SERIE R**

Transmisión telegráfica

- **SERIE S**

Equipos terminales para servicios de telegrafía

- **SERIE T**

Terminales para servicios de telemática

- **SERIE U**

Conmutación telegráfica

- **SERIE V**

Comunicación de datos por la red telefónica

- **SERIE X**

Redes de datos y comunicación entre sistemas abiertos

- **SERIE Y**

Infraestructura mundial de la información y aspectos del protocolo Internet

- **SERIE Z**

Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

3.2.1.4 Manuales ITU-T

3.2.1.4.1 Explotación

- ***Instrucciones para el servicio telefónico internacional (1993)***

Estas instrucciones incluyen la Recomendación UIT-T E.141

Artículo: E 3382 F 3381 S 3383 A 5961 **23 CHF**

3.2.1.4.2 Planificación de Redes

- *Guía para la planificación de sistemas de fibra óptica (1989)*

Artículo: E 1277 F 1278 S 1279 140 CHF

- *Manual de planificación de la transmisión (1993)*

Artículo: E 3214 F 3213 S 3215 28 CHF

- *Manual «Calidad de servicio y calidad de funcionamiento de la red» (1993)*

Artículo: E 2977 F 2976 S 2978 37 CHF

3.2.1.4.3 Directrices de implementación

- *Directrices para preparar y realizar ensayos prácticos de equipos digitales de conmutación (1987)*

Artículo: E 1116 F 1117 S 1118 20 CHF

- *Directrices para las pruebas de la RDSI (1991)*

Artículo: E 2067 F 2066 S 2068 38 CHF

- *Directrices para la realización de una red del sistema de señalización N.o 7 (1991)*

Artículo: E 1910 F 1909 S 1911 37 CHF

- *Introduction of New Technology in Local Network (1993)*

Artículo: E 3343 58 CHF

3.2.1.4.4 Planta Externa

- *Manual sobre Tecnologías de planta exterior para redes públicas (1992)*

Artículo: E 2075 F 2074 S 2076 122 CHF

- *Preservación de los postes de madera de las líneas aéreas de telecomunicación (1974)*

Artículo: E 493 F 494 S 495 23 CHF

- *Empalme de cables con cubierta de plástico (1978)*

Artículo: E 484 F 486 S 487 27 CHF

- *Empalme de conductores de cables de telecomunicación (1982)*

Artículo: E 489 F 490 S 491 47 CHF

- *Fibras ópticas para telecomunicación (1984)*

Artículo: E 1041 F 1042 S 1043 A 4721 70 CHF

- *Construcción, instalación, empalme y protección de cables de fibra óptica (1994)*

Artículo: E 3775 F 3774 S 3776 R 9590 A 5962 53 CHF

- *Aplicaciones de computadores y microprocesadores a la construcción, instalación y protección de cables de telecomunicación (1999)*

Artículo: E 14517 F 14695 S 14696 20 CHF

- *Protección de edificios de telecomunicaciones contra incendios (2001)*

Artículo: E 19255 F 19256 S 19257 28 CHF

- *Manual sobre cables terrestres sumergibles*

Artículo: E 20502 F 20503 S 20504 34 CHF

- *Adición a la sección 3 del Manual sobre Telefonometría (2001)*

Artículo: E 20261 F 20262 S 20263 12 CHF

- *Guía de uso de la publicaciones del UIT-T producidas por la Comisión de estudio 5 para satisfacer los objetivos de compatibilidad electromagnética y seguridad (2001)*

Artículo: E 20954 F 20955 S 20956 17 CHF

- *Manual sobre técnicas de medición de interferencia* ***(2001)***

Artículo: E 20506 F 20505 S 20507 38 CHF

3.2.1.4.5 Protección contra los efectos electromagnéticos

- *Puesta a tierra de las instalaciones de telecomunicación (1976)*

Artículo: E 497 F 498 S 499 41 CHF

- *Protección contra el rayo de las líneas e instalaciones de telecomunicación .*

- *Capítulos 1 a 5 (1974)*

Artículo: E 689 F 690 S 691 85 CHF

- *Capítulos 6, 7 y 8 (1978)*

Artículo: E 693 F 694 S 695 42 CHF

- *Capítulos 9 y 10 (1994)*

Artículo: E 5479 F 5478 S 5480 62 **CHF**

3.2.1.4.6 Directrices

Directrices del CCITT sobre la protección de las líneas de telecomunicación contra los efectos perjudiciales de las líneas de energía y de las líneas ferroviarias electrificadas

- Volumen I: Principios de diseño, construcción y explotación de las instalaciones de telecomunicación, de suministro de energía y de tracción eléctrica (1990)

Artículo: E 1773 F 1764 S 1782 36 CHF

- Volumen II: Cálculo de tensiones y corrientes inducidas en situaciones prácticas (1999)

Artículo: E 15034 F 15065 S 15068 160 CHF

- Volumen III: Acoplamiento capacitivo, inductivo y conductivo: teoría física y métodos de cálculo (1990)

Artículo: E 1775 F 1766 S 1784 56 CHF

- Volumen IV: Corrientes y tensiones inductoras en los sistemas de tracción eléctrica (1990)

Artículo: E 1776 F 1767 S 1785 62 CHF

- Volumen V: Tensiones y corrientes inductorasen los sistemas de transmisión y distribución de energía eléctrica (1999)

Artículo: E 15071 F 15072 S 15073 24 CHF

- Volumen VI: Peligros y perturbaciones (1990**)**

Artículo: E 1778 F 1769 S 1787 21 CHF

- Volumen VII: Medidas de protección y precauciones por razones de seguridad (1990)

Artículo: E 1779 F 1770 S 1788 21 CHF

- Volumen VIII: Dispositivos de protección (1990)

Artículo: E 1780 F 1771 S 1789 9 CHF

- Volumen IX: Métodos de prueba y aparatos de medida (1990)

Artículo: E 1781 F 1772 S 1790 84 CHF

3.2.1.4.7 Métodos de Medición

- *Manual sobre telefonometría (1993)*

Artículo: E 3771 F 3770 S 3772 86 CHF

- *Adiciones al manual sobre telefonometría (1999)*

Artículo: E 14626 F 14627 S 14628 12 CHF

- *Adiciones a la sección 2.3 del manual sobre telefonometría (2000)*

Artículo: E 458 F 471 S 474 40 CHF

3.2.1.4.8 Lenguajes formales

- *Introduction to CHILL (1993)*

Edición solamente en inglés

Artículo: E 3739 23 CHF

- *CHILL User Manual (1986)*

Edición solamente en inglés

Artículo: E 1055 31 CHF

- *CHILL Formal Definition . Volume I, Parts 1, 2, 3 (1982)*

Edición solamente en inglés

Artículo: E 1052 31 CHF

- *CHILL Formal Definition . Volume II, Part 4 (1982)*

Edición solamente en inglés

Artículo: E 1053

3.2.2 ISO

La Organización Internacional para la Estandarización (ISO) es una organización internacional no gubernamental, compuesta por representantes de los Organismos de Normalización (ONS) nacionales, que produce Normas Internacionales industriales y comerciales. Dichas normas se conocen como normas ISO.

La finalidad de dichas normas es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de:

- facilitar el comercio
- facilitar el intercambio de información
- contribuir a la transferencia de tecnologías

La Organización ISO está compuesta por tres tipos de miembros:

Miembros natos, uno por país, recayendo la representación en el organismo nacional más representativo.

Miembros correspondientes, de los organismos de países en vías de desarrollo y que todavía no poseen un comité nacional de normalización. No toman parte activa en el proceso de normalización pero están puntualmente informados acerca de los trabajos que les interesen.

Miembros suscritos, países con reducidas economías a los que se les exige el pago de tasas menores que a los correspondientes.

ISO es un órgano consultivo de la Organización de las Naciones Unidas. Coopera estrechamente con la Comisión Electrotécnica Internacional (International

Electrotechnical Commission, IEC), que es responsable de la estandarización de equipos eléctricos.

Mientras los entornos TI se vuelven cada vez más complejos, la gestión y seguridad de estas infraestructuras informáticas es cada vez más importante. Las empresas buscan ayuda en la estandarización de las mejores prácticas. Las mejores prácticas proporcionan a las empresas métodos probados por la industria para estandarizar sus procesos y gestionar sus entornos TI. Los principales estándares en esta área son la Information Technology Infrastructure Library (ITIL); el British Standard (BS15000), floreciente estándar para gestión de servicios TI basado en metodologías ITIL y la ISO 17799, estándar mundial de mejores prácticas para asegurar la información empresarial que está basado en el British Standard (BS7799).

Las empresas que deseen utilizar un enfoque basado en estándares para la estandarización de las mejores prácticas, tienen como opción varias metodologías entre ellas:

- **IT Infrastructure Library (ITIL**)—incluye definiciones de las mejores prácticas para la Gestión de Servicios. La definición se divide en dos volúmenes:

– Soporte de Servicios

– Distribución de Servicios

- **BS15000**—el primer estándar mundial para la gestión de servicios TI. Se dirige tanto a proveedores de gestión de servicios TI como a empresas que, o bien subcontratan, o bien gestionan sus propios requerimientos TI. BS15000 especifica un conjunto de procedimientos de gestión interrelacionados, basados

en gran medida en el marco de trabajo ITIL, y forma la base de una auditoria del servicio gestionado.

- **ISO 17799**—una norma global basada en el British Standard BS7799, que define las mejores prácticas para gestionar la seguridad de la información.

- **Gestión de la Seguridad ITIL—**los procedimientos de las mejores prácticas para asegurar la infraestructura TI gestionada, que están íntimamente relacionados con el uso de las mejores prácticas ISO 17799.

Europeas

Introducción a la Política de Normalización en la Unión Europea

El Libro Verde de la Comisión sobre el desarrollo de la normalización europea: medidas para acelerar la integración tecnológica en Europa, de 10 de diciembre de 1990 [COM (90)456], recoge una serie de propuestas dirigidas a la industria, a los organismos de normalización y a las Administraciones para que cooperen y presten un firme apoyo para dar un mayor impulso a la estrategia de la normalización europea con objeto de acelerar la creación del mercado interior.

En respuesta a estas propuestas de la Comisión, el Consejo adoptó, con fecha 18 de junio de 1992, una Resolución relativa a la función de la normalización en el marco de la economía europea [DO C 173/1] que, entre otras cosas, señala que, si bien la organización de la normalización europea se basa en una cooperación voluntaria entre las partes interesadas, esta ha de servir al interés público.

Es por ello que, ante la urgencia de disponer de normas de alta calidad, cuyo uso pudiera servir de instrumento de la integración económica e industrial, dicha resolución considera que hay que evitar una fragmentación de los trabajos europeos de normalización y, por tanto, recomienda a los organismos europeos de normalización que refuercen su coordinación y adopten medidas para aumentar su eficacia a corto plazo.

Específicamente, en materia de telecomunicaciones, con la llegada de la libre competencia tanto en servicios como en infraestructuras, se establece el principio de contar con normas europeas y del carácter voluntario de las mismas a excepción de aquellos casos en los que se considere necesario hacer obligatorio su cumplimiento para salvaguardar el interés general.

Así, los equipos terminales deben satisfacer una serie de requisitos esenciales en cuanto a seguridad, compatibilidad electromagnética, uso efectivo del espectro de radiofrecuencias e interfuncionamiento.

A este respecto, hay que recordar que, por definición, el cumplimiento de las especificaciones técnicas contenidas en una norma siempre tienen un carácter voluntario mientras que el cumplimiento de aquellas especificaciones técnicas contenidas en una reglamentación son obligatorias.

Es por ello que, para garantizar el cumplimiento de los requisitos esenciales y para que los fabricantes puedan demostrar más fácilmente la conformidad con dichos requisitos, conviene disponer de normas europeas armonizadas que los Estados miembros deberán incorporar a sus legislaciones nacionales.

Una norma armonizada es una especificación técnica (norma europea y documento de armonización) adoptada por uno de los organismos europeos de normalización reconocidos basándose en un mandato de la Comisión de acuerdo con lo dispuesto en la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, que

instaura un mecanismo de transparencia reglamentaria para los servicios de la sociedad de al información, y modifica la Directiva 98/34/CE por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas (Directiva por la que se codifica el procedimiento de notificación 83/189).

Los organismos europeos de normalización reconocidos a tal efecto son:

- **CEN :** Comité Europeo de Normalización
- **CENELEC:** Comité Europeo de Normalización Electrotécnica
- **ETSI :** Instituto Europeo de Normas de Telecomunicaciones

3.2.3 CEN/CENELEC

El Comité Europeo de Normalización (CEN) desarrolla trabajos de Normalización que cubren todos los sectores técnicos con excepción del campo electrotécnico, que es competencia del Comité Europeo de Normalización Electrotécnica (CENELEC).

El papel de ambas organizaciones, sin ánimo de lucro, es crear normas europeas que fomenten la competitividad de la industria europea a nivel mundial y ayuden a crear el mercado interior europeo.

Para realizar esta actividad, ambos organismos fomentan la adopción de normas ISO y CEI.

- **Objetivo**

Los objetivos básicos de CEN/CENELEC son los siguientes:

Preparar nuevas normas Europeas o documentos de armonización sobre aquellos temas en los que no existen normas Internacionales o nacionales.

Promover la implantación en Europa de las normas desarrolladas por ISO o por CEI

- **Miembros**

Los Comités miembros nacionales del CEN/CENELEC son los Organismos nacionales de normalización pertenecientes tanto a los Estados miembros de la UE (AENOR en España) como de la EFTA, así como la República Checa.

- **Estructura**

La elaboración de las Normas Europeas se realiza en estructuras técnicas análogas a las de ISO y CEI.

3.2.3.1 Documentos normativos CEN/CENELEC

- Normas Europeas (ENs) de obligado cumplimiento por los miembros y que se adopta como norma nacional y aprobada mediante un procedimiento de voto ponderado

- Norma experimental europea (ENVs) documento elaborado por los miembros para su aplicación provisional en aquellos campos técnicos donde exista un elevado grado de innovación tecnológica, una urgente necesidad de orientación o donde estén implicadas la seguridad de las personas o de los bienes.

- Otros documentos e informes

3.2.4 ETSI

3.2.4.1 Introducción

Instituto Europeo de Normas de Telecomunicaciones

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) es un organismo sin ánimo de lucro creado al objeto de disponer del foro adecuado para la elaboración de las normas de telecomunicación que faciliten la estandarización del sector, y por lo tanto el avance hacia el Mercado Único Europeo. En el ETSI participan como miembros no sólo las Administraciones, sino también los operadores de red, la industria, los centros de investigación y los usuarios de los servicios de telecomunicación.

A continuación se hace una breve descripción del ETSI, sus objetivos, miembros, estructura, documentos normativos, procesos de aprobación de normas y de la representación de la Administración Española en el ETSI.

- **Objetivo**

Los objetivos del ETSI se reducen básicamente a la elaboración y mantenimiento/actualización de prenormas y de normas técnicas a nivel europeo en los siguientes campos:

- Telecomunicaciones.
- Áreas comunes existentes entre las telecomunicaciones y las tecnologías de la información.

- Áreas comunes existentes entre las telecomunicaciones y los sistemas de radiodifusión y televisión.

Es, por tanto, el ETSI la organización clave en el contexto europeo para la elaboración de normas tanto en el sector de las telecomunicaciones como para la convergencia de este sector con los de tecnologías de la información y audiovisual.

- **Miembros**

Pueden ser miembros del ETSI: Administraciones, operadores de redes públicas, fabricantes, organizaciones de usuarios y organismos de investigación. La participación puede ser a título individual o formando parte de grupos. Asimismo, el ETSI admite miembros observadores con ciertas limitaciones en sus derechos.

- **Estructura**

El ETSI está estructurado en los siguientes órganos de gobierno:

a) Asamblea General

Está formada por todos los miembros, agrupados por delegaciones nacionales. La UE y la EFTA podrán estar en las Asambleas a título de consejeros, pero sin derecho a voto. Los miembros de pleno derecho y los asociados pueden votar en todas las cuestiones (de acuerdo al artículo 11.2 del Reglamento interno del Instituto). Cuando haya que determinar la existencia de quórum, tan sólo se considerará a los miembros de pleno derecho. La Asamblea general es el órgano supremo del Instituto en la toma de decisiones y se responsabiliza, entre otras, de las siguientes tareas:

- Determinar la política general del Instituto.

- Adoptar los presupuestos anuales y aprobar los estatutos financieros.

- Aprobar el informe anual.

- Elegir los cargos más representativos del Instituto y nombrar a los miembros del Consejo.

- Aprobar los Estatutos y Reglamentos internos y de funcionamiento del Instituto.

- Ratificar los acuerdos con otras organizaciones.

b) Secretaría

Está formada por el Director y su personal, siendo responsable entre otros temas de:

- Asignación de recursos.

- Preparación de los esquemas de trabajos de acuerdo con las directrices fijadas por la Asamblea General.

- Preparación de presupuestos.

c) Consejo

Está formado por un número reducido personas de reconocido prestigio y valía en el campo de las Telecomunicaciones que representan a todas las organizaciones miembros del Instituto, siendo elegidas por éstas entre los candidatos que ellas mismas proponen. Destacan, entre otras, las siguientes funciones delegadas:

- Asesorar a la Asamblea general acerca de las políticas generales de normalización y mantener actualizados los grados de interés, la eficacia, los plazos y la calidad de los planes o acuerdos de normalización.

- Tomar decisiones sobre el programa de trabajo del Instituto con revisiones periódicas, incluyendo la creación o desaparición de grupos técnicos (TC, EP y EPP), la aprobación de sus mandatos, y la aprobación, mantenimiento y aplicación de los programas técnicos de trabajo.

- En el marco económico fijado por la Asamblea general, tomar decisiones relativas a los programas de trabajo financiado y voluntario, incluyendo la creación y asignación de recursos financieros para los grupos de tareas especiales.

- En el período comprendido entre convocatorias de la Asamblea general, actuar en nombre de ésta en la toma de aquellas decisiones que le hayan sido delegadas explícitamente.

d) Organización Técnica

Constituye el foro de discusión técnico y es la encargada de preparar los programas de trabajo y los productos normativos del Instituto. Los órganos técnicos son los centros primarios de toma de decisiones en aquellas cuestiones incluidas en sus mandatos ("Terms of Reference"). Se distinguen tres tipos de órganos técnicos:

Comités técnicos (Technical Committee, TC)

Encargados de la elaboración de normas de carácter general u "horizontal" por su aplicabilidad a diversos campos en las redes y servicios de telecomunicaciones:

- TC AT (Access and Terminals), sobre terminales y acceso a redes de comunicaciones.

- ECMA TC32 (Communication, Networks & Systems Interconnection), sobre Comunicaciones, redes y sistemas de interconexión

- JTC Broadcast (Joint Technical Committee on Broadcast), Comité técnico conjunto de EBU, CENELEC y ETSI sobre difusión

- TC EE (Environmental Engineering), sobre cuestiones de ingeniería relativas al entorno

- TC ERM (EMC and Radio Spectrum Matters), sobre cuestiones de compatibilidad electromagnética y espectro radioeléctrico

- TC HF (Human Factors) sobre factores humanos

- TC MSG (Mobile Standards Group) sobre normas relativas a sistemas móviles

- TC MTS (Methods for Testing & Specification), sobre métodos de pruebas y especificaciones

- TC SAFETY (Telecommunications Equipment Safety), sobre seguridad física en equipos y sistemas de telecomunicaciones

- TC SEC (Security) , sobre seguridad relativa a la información

- TC SES (Satellite Earth Stations & Systems), sobre estaciones y sistemas terrenos de satélite.

- TC SPAN (Services and Protocol for Advanced Networks), sobre protocolo y servicios de redes avanzadas
- TC STQ (Speech processing Transmission&Quality), sobre procesamiento transmisión y calidad de voz
- TC TM (Transmission and Multiplexing), sobre transmisión y multiplaje
- TC TMN (Telecommunications Management Networks), sobre gestión de redes de telecomunicaciones

Proyectos ETSI (ETSI Project, EP)

Encargados de la elaboración o promoción de normas específicas para un área o aspecto determinado de las telecomunicaciones, con vistas a la consecución, en un periodo de tiempo predeterminado, de un conjunto coherente de normas que posibiliten la implantación de un nuevo servicio, red o sistema de telecomunicaciones. Para lograr este objetivo se alienta a que "subcontraten" la elaboración de las normas pertinentes de carácter horizontal en los Comités Técnicos responsables de las áreas respectivas.

- EP BRAN (Broadband Radio Access Networks), sobre redes de acceso radio de banda ancha
- EP DECT (Digital Enhanced Cordless Telecommunication), sobre telecomunicaciones digitales inalámbricas mejoradas
- EP M-COMM (Mobile Commerce), sobre comercio en sistemas móviles
- EP SCP (Smart Card Platform), sobre plataforma de tarjetas inteligentes

- EP PLT (Power Line Telecommunications), sobre telecomunicaciones a través de líneas de energía eléctrica
- EP TETRA (Terrestrial Trunked Radio), sobre sistemas de radio troncales
- EP TIPHON (Telecommunications and Internet Protocol Harmonization Over Network), sobre armonización de protocolos entre redes de telecomunicaciones e Internet

3) **Proyectos del ETSI en colaboración (ETSI Partnership Project,):** que son actividades desarrolladas en cooperación con otro organismo ajeno al Instituto, cuando la citada colaboración no es posible dentro de las modalidades de Proyectos del ETSI (EP) o de los Comités técnicos (TC).

3GPP (Third Generation Partnership Project), sobre sistemas móviles de tercera generación. Tiene cuatro subproyectos:

- TSG- CN (Core Network)
- TSG- RAN (Radio Access Networks)
- TSG-SA (Services and System Aspects)
- TSG- T (Terminals)
- PSPP (Public Safety Partnership Project), sobre sistemas móviles de banda ancha para aplicaciones de seguridad pública. Tiene cuatro subproyectos:
- PSPP- CN (Core Network)

- PSPP- RAN (Radio Access Networks)
- PSPP-SA (Services and System Aspects)
- PSPP- T (Terminals)

E) Comités especiales:

Se encargan de tareas concretas: Comité de finanzas, Grupo de promoción de normas europeas de telecomunicaciones (ETSAG), Comité conjunto ECMA/ETSI, Grupo de coordinación operativo (OCG)

3.2.4.2 Tipos de documentos normativos elaborados por el ETSI

Entre el tipo de documentos generados por el ETSI en las series de telecomunicaciones están:

- TS, Especificación técnica: contiene las disposiciones normativas aprobadas para su publicación por un órgano técnico del ETSI (un comité técnico, un equipo de proyecto ETSI o un proyecto del ETSI en colaboración).
- TR, Informe técnico: principalmente contiene elementos informativos que han sido aprobados para su publicación por un órgano técnico del ETSI (un comité técnico, un equipo de proyecto ETSI o un proyecto del ETSI en colaboración).
- ES, Norma ETSI: contiene disposiciones normativas que han sido aprobadas para su publicación mediante el procedimiento de aprobación de los miembros del Instituto.

- EG, Guía ETSI: principalmente contiene datos informativos que han sido aprobados para su publicación mediante el procedimiento de aprobación de los miembros del Instituto.

- EN, Norma Europea: contiene disposiciones normativas que han sido aprobadas para su publicación en un proceso en el que participan los organismos nacionales de normalización o las delegaciones nacionales en el ETSI; ello conlleva la obligatoriedad de una transposición nacional con los períodos de "statu quo" correspondientes.

- Norma Armonizada: norma europea EN cuyo proyecto le ha sido confiado al ETSI en virtud de un mandato de la Comisión Europea bajo la Directiva 98/34/CE (la última modificación de la Directiva 83/189/CEE) y que se ha redactado teniendo en cuenta los requisitos esenciales de la Directiva de Nuevo Enfoque y cuya referencia se ha publicado posteriormente en el Diario Oficial de las Comunidades Europeas.

- SR, Informe Especial: cualquier otro producto normativo del ETSI que contenga información de utilidad y disponible al público para los propósitos de referencia. Ejemplos: informaciones acerca de declaraciones sobre Derechos de Propiedad Intelectual (IPR), las conclusiones de los comités especiales, etc.

3.2.4.3 Elaboración, aprobación e implementacion de normas europeas

Cada Delegación Nacional de Normalización (AENOR en el caso de España) reconocida para llevar a cabo el proceso de Información Pública, establecer la posición nacional para el voto, para los requisitos de trasposición, y para todo lo referente a la derogación de las normas.

Existe la obligación aceptada por el Organismo Nacional de Normalización y por los miembros de ETSI de no realizar actividad de Normalización alguna que pueda perjudicar la preparación de una EN.

Asimismo, el Organismo Nacional de Normalización no podrá publicar una norma nueva no revisada que no esté completamente en acordancia con las ENs existentes. Esta obligación no es infringida si:

- el Organismo Nacional de Normalización publica una norma nacional, ya adoptada, antes de tres meses desde que ETSI expresa su intención del elaborar una EN sobre el mismo tema.
- el Organismo Nacional de Normalización publica una norma nacional adoptando una Recomendación UIT, o norma ISO O CEI, sin cambio alguno.

Antes de que un borrador de EN se remita para aprobación por parte de ETSI, éste debe haber tenido un proceso de Información Pública realizado por el Organismo Nacional de Normalización. Las propuestas y comentarios que reciben se consolidan y remiten a la Secretaría del ETSI.

Las EN pueden tener un procedimiento de aprobación en una sola vuelta, en el que la información Pública y votación se combinan. Generalmente, este proceso es utilizado cuando la EN procede de una norma previa ES que no sufre modificación, salvo de carácter confidencial. El procedimiento de aprobación en dos vueltas tiene separadas en el tiempo la fase de Información Pública y la del voto.

3.2.4.4 Elaboración , aprobación, e implementación de normas ETSI (ES) y guías ETSI (EG)

ESs y EGs son documentos elaborados por los órganos técnicos (TC, EP y EPP) que pueden ser publicados por ETSI previa aprobación en votación individual ponderada de los miembros de pleno derecho y miembros asociados.

3.2.4.5 Representacion de la administración española en el ETSI

Desde su fundación, la Administración Española ha estado representada oficialmente en el Instituto. Esta representación es ejercida por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información como miembro de pleno derecho, incluyéndose asimismo en sus presupuestos la liquidación de la contribución que, como administración de telecomunicaciones, corresponde pagar al Ministerio de Ciencia y Tecnología.

La Comisión de las Comunidades Europeas en su "Comunicación al Consejo relativa a la normalización comunitaria", solicita al Consejo que inste a los países miembros para que procedan al establecimiento de los organismos nacionales que se ocupen de la transposición de las normas, así como de observar los períodos prenormativos (statu quo) a que se refería el artículo 14 del Reglamento interno del ETSI (recogidas en su artículo 13). La comunicación formal a la Comisión de dichos organismos, así como de sus reglas de funcionamiento, por parte de los países miembros es un requisito imprescindible para que la Comisión reconozca al ETSI como organismo europeo de normalización y lo incluya en la Directiva 98/34/CE del Parlamento y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas.

En base a lo anterior, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, junto con la Asociación Española de Normalización y Certificación (AENOR), participa en la elaboración y transposición de las normas técnicas e informes emanados del ETSI, convirtiéndolos en normas nacionales.

3.3 Normas de evaluación y certificación

Estadounidenses

3.3.1 TCSEC

Libro naranja

El TCSEC (Trusted Computer System Evaluation Criteria), también llamado libro naranja, surgió a finales del 1985 con el objetivo de servir de referencia para la clasificación y evaluación de la fiabilidad/seguridad de sistemas computacionales, debido a la aparición de una directiva del departamento de defensa de EEUU en el que indicaba que todas sus partes debían cumplir con dichos criterios para su uso.

TCSEC tiene por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

Para clasificar los sistemas utiliza una nomenclatura que varía de sistemas tipo D (aquellos que no cumplen con los requisitos mínimos de seguridad) hasta el A (sistemas cuya protección ha sido verificada matemáticamente).

3.3.1.1 Requisitos Fundamentales de la Seguridad en Cómputo

Cualquier discusión sobre seguridad en cómputo necesariamente empieza con una definición de sus requisitos básicos, es decir, realmente qué significa el llamar a un sistema informático "seguro".

En general, un sistema seguro controlará, a través del uso de características específicas de seguridad, el acceso a la información, de forma tal, que solamente los individuos autorizados correctamente, o los procesos que obtienen los permisos adecuados, tendrán acceso para leer, escribir, crear, modificar o eliminar la información.

Se tienen seis requisitos fundamentales, los cuales se derivan de esta declaración básica; cuatro de ellos parten de la necesidad de proporcionar un control de acceso a la información y los dos restantes de cómo puede obtenerse una seguridad demostrable, logrando así un sistema informático confiable.

- **Requisito 1**

POLÍTICA DE SEGURIDAD

Debe existir una política de seguridad explícita y bien definida reforzada por el sistema. Identificados los eventos y los objetos, debe haber un conjunto de reglas que son utilizadas por el sistema para determinar si un evento dado se puede permitir para acceder a un objeto específico. Los sistemas informáticos de interés deben hacer cumplir una política obligatoria de seguridad, en la cual puedan implementarse eficientemente reglas del acceso para manejo de información sensitiva (p.e. clasificaciones) estas reglas deben de incluir requisitos tales como: Ninguna persona que carezca de los permisos apropiados obtendrá el acceso a la información clasificada. Además, los controles de seguridad discrecional se requieren para asegurar que solamente los usuarios o los grupos seleccionados de usuarios puedan obtener el acceso a los datos.(p.e., basarse en una necesidad de conocimientos específicos).

- **Requisito 2**

MARCAS

El control de acceso por etiquetas debe de estar asociado a los objetos. Para controlar el acceso a la información almacenada en una computadora, según las reglas de una política obligada de seguridad, debe de ser posible el marcar cada objeto con uno una etiqueta que identifique confiablemente el nivel de la sensibilidad del objeto (p.e.,

clasificación), y/o los modos de obtener acceso y acordar quien puede tener acceso potencial al objeto.

- **Requisito 3**

IDENTIFICACIÓN

Los eventos individuales deben de ser identificados. Cada acceso a la información debe ser registrado teniendo como base quién está teniendo acceso a la información y qué autorización posee para ocupar cierta clase de información. La información de la identificación y la autorización debe ser administrada con seguridad por el sistema informático y asociar cierta seguridad a cada elemento activo que realice una cierta acción relevante en el sistema.

- **Requisito 4**

RESPONSABILIDAD

Las auditorias de la información deben ser selectivamente guardadas y protegidas de las acciones que puedan afectar la seguridad y de testa forma poder rastrear al responsable. Un sistema confiable debe tener la capacidad de registrar la ocurrencia de acontecimientos relevantes sobre seguridad en una bitacora auditable. Además de poseer la capacidad de seleccionar los eventos a auditar para ser registrados, es necesario para reducir al mínimo el costo de la revisión y permitir un análisis eficiente. Este tipo de registros o bitácoras, deben de estar protegidos contra la modificación y la destrucción no autorizada, y deben permitir la detección y la investigación posterior de las violaciones de seguridad.

- **Requisito 5**

ASEGURAMIENTO

El sistema informático debe contener los mecanismos de hardware/software que puedan ser evaluados independientemente para proporcionar una seguridad suficiente que el sistema haga cumplir los requisitos 1 a 4 mencionados anteriormente.

Para asegurar que los requisitos de política de seguridad, marcas, identificación, y responsabilidad de la seguridad son hechos cumplir por un sistema de cómputo, deben ser identificados como una colección unificada de hardware y software que controle y ejecute esas funciones. Estos mecanismos son típicamente incluidos en el sistema operativo y se diseñan para realizar las tareas asignadas de una manera segura. La base para confiar en tales mecanismos del sistema operativo, radica en su configuración operacional, la cual debe ser claramente documentada a fin de hacer posible el examinar independientemente los eventos para su evaluación.

- **Requisito 6**

PROTECCIÓN CONTINUA

Los mecanismos de seguridad que hacen cumplir estos requisitos básicos, se deben de proteger continuamente contra cambios no autorizados o modificaciones que traten de alterarlos. Ningún sistema de cómputo puede ser considerado verdaderamente seguro si los mecanismos que hacen cumplir las políticas de seguridad, están sujetos a modificaciones no autorizadas. El requisito de protección continua tiene implicaciones directas a través del ciclo de vida de los sistemas.

3.3.1.2 Propósito del Libro Naranja.

De acuerdo con el texto mismo, el criterio de evaluación se desarrolla con 3 objetivos **básicos:**

- **Medición:**

Para proporcionar de elementos cuantificables al Departamento de Defensa (DoD) con los cuales poder evaluar el grado de confianza que se puede tener en los sistemas informáticos seguros, para el proceso de clasificación de información sensitiva.

El proveer a los usuarios con un criterio con el cual se evalúe la confianza que se puede tener en un sistema de cómputo para el procesamiento de la seguridad o clasificación de información sensitiva.

Por ejemplo, un usuario puede confiar que un sistema B2 es más seguro que un sistema C2.

- **Dirección:**

Para proporcionar un estándar a los fabricantes en cuanto a las características de seguridad que deben de implementar en sus productos nuevos y planearla con anticipación, para aplicarla en sus productos comerciales y así ofrecer sistemas que satisfacen requisitos de seguridad (con énfasis determinado en la prevención del acceso de datos) para las aplicaciones sensitivas.

- **Adquisición**

El proporcionar las bases para especificar los requerimientos de seguridad en adquisiciones determinadas.

Más que una especificación de requerimientos de seguridad, y tener vendedores que respondan con una gama de piezas. El libro naranja proporciona una vía clara de especificaciones en un juego coordinado de funciones de seguridad. Un cliente puede estar seguro que el sistema que va a adquirir fue realmente verificado para los distintos grados de seguridad.

A continuación se enumeran las siete clases:

1.- Sistemas D (Protección Mínima):

En esta clasificación caen todos aquellos sistemas que no cumplen con todos los requisitos para entrar en una clasificación superior.

2.- Sistemas C (Protección Discreta):

2.1. C1: Protección de seguridad discreccional.

El sistema debe definir y controlar el acceso de los usuarios a los objetos. También debe permitir a los usuarios controlar el acceso a dichos objetos a través de listas de control de accesos (dueño, grupos y otros). Para ello se requiere un sistema de autentificación vía contraseña para identificar a los usuarios. También es necesario que el código y las estructuras de datos corran en un dominio distinto del de los usuarios (ring 0).

2.2.- C2: Protección de acceso controlado

Se necesita además de lo contenido en el C1 un aumento de la granularidad, es decir, extender dueño/grupo/otros a listas de control de accesos individuales y aumentar la flexibilidad. El sistema debe ser capaz de registrar los accesos de los usuarios a los objetos del sistema y proteger dichos registros contra accesos no autorizados. Política de negación por defecto (el sistema no debe permitir el acceso antes de que su dueño asigne los permisos)

3.- Sistemas B (Protección mandataria):

Todos los sistemas B requerirán de las capacidades de los C y necesitarán del uso de etiquetados de sensibilidad basado en el modelo de Bell-LaPadula. Empezamos a hablar de sistemas fiables. A indicar que el modelo de Bell-LaPadula solo protege la confidencialidad de los datos y no su integridad (modelo BIBA) pero es en el que se basa en exclusiva el TCSEC. Por lo tanto, un sistema que utilice los dos métodos será por defecto más seguro que uno que utilice tan sólo el modelo de Bell-LaPádula aunque la calificación obtenida en el TCSEC será la misma.

3.1.- B1: Protección mediante etiquetas

Se le asigna a los objetos una etiqueta con un nivel de sensibilidad y a los sujetos otra con su nivel de seguridad sólo modificable ambos por el TCB (no-discreccional). El acceso a la información está controlado por ella. Aunque el Control de Acceso Discreccional permita el acceso a un recurso, no garantiza su disponibilidad si el MAC no lo confirma.

3.2.- B2: Protección estructurada.

Se implementa una política de menor privilegio en el kernel, se realiza un modelo formal de seguridad. Todos los objetos, incluyendo dispositivos y canales de entrada/salida están etiquetados.

3.3.- B3: Dominios de seguridad

Rediseño del TCB, debe ser lo más pequeño posible, cualquier código innecesario debe ser excluido de él, además debe ser muy modular. Se amplían las capacidades de registro para señalar eventos relacionados con la seguridad.

4.- Sistemas A (Protección verificada):

4.1. A1: Diseño verificado

Funcionalmente es equivalente a un sistema B3, el sistema y su modelo matemático han sido completamente analizados y probados.

El Libro Naranja fue desarrollado por el **NCSC** (**National Computer Security Center**) de la **NSA** (**National Security Agency**) del Departamento de Defensa de EEUU. Actualmente, la responsabilidad sobre la seguridad de SI la ostenta un organismo civil, el **NIST** (**National Institute of Standards and Technology**).

El TCSEC establece el concepto de **monitor de referencia**, como responsable de autorizar las relaciones de acceso permitidas entre sujetos y objetos. En la Figura 1 se ilustra su función.

La implementación de este concepto se denomina mecanismo de validación de referencias. Para este mecanismo el TCSEC requiere:

- Debe ser resistente a ataques.
- Debe mediar todos los intentos de acceso.
- Debe ser suficientemente pequeño para poder ser analizado y probado.

Un sistema diseñado y realizado para verificar estos criterios se dice que implementa un núcleo de seguridad. Tales sistemas alcanzan las mayores cotas de seguridad.

Muchos sistemas implementan el mecanismo de validación de referencias como parte de un mecanismo más general (por ejemplo, todo el sistema operativo) por lo que no satisfacen el último de los requisitos anteriores. Para comprender a éstos, que son mayoría, el TCSEC define el “Trusted Computing Base” (TCB) como aquella parte del

sistema que contiene todos los elementos (aunque quizás no sólo ellos) responsables de la seguridad. Aunque el TCB puede ser extraordinariamente grande y complejo, el TCSEC recomienda su simplicidad.

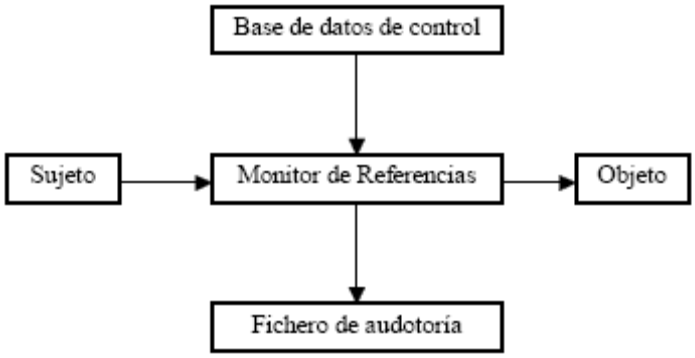


Figura 1. Mediación del monitor de referencias entre sujeto y objeto.

Europeos

3.3.2 ITSEC/ ITSEM

3.3.2.1 Introducción

En mayo de 1990 Francia, Alemania, Los Países Bajos y el Reino Unido publicaron los Information Technology Security Evaluation Criteria (ITSEC) basados en los trabajos realizados en estos países. ITSEC se ha desarrollado intensamente hasta la versión 1.2, que data de junio de 1991. Precursor de este producto fue el Trusted Computer System Evaluation Criteria, generalmente conocido por TCSEC o 'Libro Naranja', publicado inicialmente en 1983 y utilizado para la evaluación de productos por el Departamento de Defensa de los Estados Unidos. Para situar ITSEC en el contexto de la SSI hay que

partir del hecho de que la información en sistemas de TI tiene que estar protegida contra amenazas que conduzcan a daños en los activos. Estas amenazas pueden ser deliberadas (ataques) o inadvertidas (errores o fallos). Para reducir el riesgo hay que seleccionar unas contramedidas específicas, que pueden ser de naturaleza física, relativas al personal, organizativas o técnicas. Las contramedidas técnicas son las funciones y mecanismos de seguridad del propio sistema de TI (p.ej.: control de accesos, recuperación de errores). Las restantes contramedidas, relativas a los aspectos físicos, de personal u organizativos constituyen el grupo de contramedidas no técnicas. Pues bien, la evaluación de ITSEC se refiere principalmente a contramedidas técnicas.

Luego de la publicación de ITSEC, los cuatro Estados Miembros autores de los criterios colaboraron para producir un primer borrador de una Metodología armonizada que acompañara a estos criterios. De esta manera y con el apoyo de SOGIS, surgió ITSEM, cuya versión 1.0 data de septiembre de 1993 . El objetivo específico de ITSEM es asegurar que existe un conjunto armonizado de métodos de evaluación que complementa a ITSEC.

Una importante limitación a tener en cuenta en ITSEC/ITSEM es que la evaluación se refiere a la seguridad de productos de TI y (en alguna medida) de sistemas de TI. Por el momento, no cubren la evaluación de servicios y aplicaciones. Ciñéndonos al caso de los servicios de telecomunicación, la idea de proporcionar un servicio de seguridad como parte de un servicio de telecomunicación dará lugar a que todas las entidades involucradas en la provisión del servicio de telecomunicación, también tendrán que participar en la provisión del servicio de seguridad. Puede incluso que se necesiten entidades adicionales, como una TTP para gestión de claves o servicios de autenticación.

Todas estas entidades utilizarán sistemas y productos para proporcionar su parte del servicio de telecomunicación/seguridad. El servicio total, por consiguiente, se proporciona a través de la interacción de todas las entidades.

El esquema que en la actualidad incluye ITSEC/ITSEM está orientado, como hemos dicho más arriba, a la evaluación técnica de productos y sistemas. No cubre medidas organizativas, de personal, administrativas o de tipo físico no relacionadas con la TI. Pero muchos servicios de seguridad en telecomunicaciones descansarán no sólo en medidas técnicas de seguridad, sino también en otros controles de los mencionados. Para ello, es claro que se precisen una extensión del esquema de evaluación de ITSEC/ITSEM para cubrir estos aspectos.

Por todo esto, la integración de todas las medidas de seguridad debe verificarse a fin de garantizar su consistencia, integridad y eficacia. Si este es el caso de los servicios, la situación se agrava con las aplicaciones, cuya seguridad es el verdadero interés del usuario, dado que la utilización de productos, sistemas y servicios seguros es condición necesaria, pero no suficiente para que el usuario vea satisfechos sus requisitos de protección de la aplicación.

ITSEC e ITSEM son documentos técnicos, dirigidos fundamentalmente a los actores que participan en una evaluación (en primer lugar, los evaluadores, pero también los patrocinadores y certificadores), aunque también tienen interés para suministradores, desarrolladores, acreditadores de sistemas y usuarios. Desde la perspectiva del usuario, adoptada en esta comunicación, son documentos de difícil lectura. Por ello, vamos a tratar de resumir a continuación algunos de los conceptos clave manejados.

El primero de estos conceptos es el de Objetivo de Evaluación (Target of Evaluation: TOE). Recibe este nombre un producto o sistema de TI sujeto a una evaluación de seguridad. Un TOE puede construirse a partir de varios componentes. Algunos no contribuirán a satisfacer los objetivos de seguridad del TOE; otros sí. Estos últimos se denominan ejecutores de la seguridad (security enforcing). También puede haber entre los primeros algunos componentes que, sin ser ejecutores de la seguridad, deben operar correctamente para que el TOE ejecute la seguridad; éstos reciben el nombre de

relevantes para la seguridad (security relevant). La combinación de los componentes ejecutores de la seguridad y relevantes para la seguridad se denomina a menudo la Base Informática Segura (Trusted Computing Base: TCB).

Para que un TOE satisfaga sus objetivos de seguridad debe incorporar funciones ejecutoras de la seguridad apropiadas, cubriendo áreas tales como control de accesos, auditoría y recuperación de errores. Estas funciones deben definirse de manera clara y comprensible tanto para el patrocinador como para el evaluador independiente. Pueden especificarse individualmente o mediante referencia a unas clases de funcionalidad predefinidas. ITSEC incluye diez ejemplos de clases de funcionalidad, de las cuales cinco corresponden estrechamente con los requisitos de confidencialidad de TCSEC.

Otras clases de funcionalidad predefinidas hacen énfasis en diferentes aspectos de la seguridad. Así, la clase F-IN está orientada a TOEs con altos requisitos de integridad en programas y datos (p.ej: bases de datos); F-AV establece altos requisitos de disponibilidad, por lo que resulta de aplicación en el control de procesos de fabricación, etc.

ITSEC distingue entre la confianza en la corrección de la implantación de funciones y mecanismos ejecutores de la seguridad y confianza en su efectividad. La evaluación de efectividad establece si las funciones y mecanismos ejecutores de la seguridad proporcionadas en el TOE satisfarán los objetivos de seguridad establecidos. El TOE es evaluado en relación con su adecuación a la funcionalidad, integración de funcionalidad, consecuencias de vulnerabilidades y facilidad de uso. Además se evalúa la fortaleza de los mecanismos del TOE, de acuerdo con tres niveles: básico, medio y alto.

La evaluación de corrección se orienta a conocer si las funciones y mecanismos ejecutores de la seguridad están correctamente implementados. ITSEC define siete niveles de evaluación de E0 a E6, representando niveles crecientes de confianza en la

corrección. E0 representa una confianza inadecuada. E1 representa un punto entrada en lo que se refiere a confianza y E6 es el nivel más alto de confianza. La corrección se contempla desde el punto de vista de construcción del TOE, considerando tanto el proceso de desarrollo como el ntorno de desarrollo, y también desde el punto de vista de la operación del TOE.

Los criterios establecidos en ITSEC permiten una selección de funciones de seguridad arbitrarias, y definen siete niveles de evaluación con una confianza creciente en la capacidad del TOE para alcanzar su objetivo de seguridad. Así, estos criterios pueden aplicarse para cubrir una gama más amplia de productos y servicios que en el caso del TCSEC.

Aunque en sentido general no se puede hablar de una relación directa entre los niveles de evaluación de ITSEC con los requisitos de confidencialidad de las clases de TCSEC, dado que ITSEC contiene unos cuantos requisitos que no aparecen explícitamente en TCSEC, en ITSEC se ha intentado establecer la siguiente correspondencia con las claves de TCSEC (Tabla 1) donde en la columna relativa a la tabla siguiente:

ITSEC		**TCSEC**
E0	<->	D
F-C1, E1	<->	C1
F-C2, E2	<->	C2
F-B1, E3	<->	B1
F-B2, E4	<->	B2
F-B3, E5	<->	B3
F-B3, E6	<->	A1

TOTAL Serio Moderado

Menor

ITSEC se ha situado a la izquierda de cada uno de los niveles de evaluación (E1 a E6) una clave de funcionalidad predefinida en los criterios. Así F-C1 es una clase de funcionalidad derivada de los requisitos de funcionalidad de la clase C1 de ITCSEC: proporciona control de accesos discrecional, y análogamente en los demás casos.

3.3.2.2 Criterios de evaluación de la seguridad

3.3.2.2.1 ITSEM: Information Technology Security Evaluation Manual.

Basada en la versión 1.0 del manual, editada en 1993

Objetivo especifico: asegurar la existencia de un conjunto armonioso de métodos de evaluación que completen los criterios ITSEC.

Esta formado por 6 partes:

- **Marco para la seguridad de las TI:** contexto y argumentos sobre la seguridad, la evaluación, la certificación de las TI. Y la homologación de los sistemas. Parte de carácter general destinada a los responsables.
- **Esquema de evaluación y certificación:** establecimiento y funcionamiento. Características generales del proceso de certificación y su organización.
- **Filosofía, conceptos y principios de los ITSEC:** para una mejor comprensión técnica.
- **Proceso de evaluación:** parte clave para los implicados en la evaluación. Descripción de la evaluación en términos de datos, acciones y resultados.

- **Relación con ITSEC:** ejemplo de la manera en que los criterios ITSEC pueden aplicarse a la evaluación de sistemas y productos.

- **Guía de ayuda a las partes implicadas en la evaluación:** Preparación de los datos y utilización de los resultados de la evaluación.

3.3.2.2.2 ITSEC: Information Technology Security Evaluation Criteria

La evaluación ITSEC se refiere principalmente a contramedidas técnicas .

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

La evaluación de un predeterminado objeto de evaluación se refiere siempre a una pareja formada por una CLASE DE FUNCIONALIDAD y por UN NIVEL DE SEGURIDAD:

- La pareja F-C1, E1 corresponde a la clase C1 estadounidense.

ITSEC incluye diez ejemplos de clases de funcionalidad, de las cuales cinco corresponden estrechamente con los requisitos de confidencialidad de TCSEC:

- Compatibilidad con TCSEC: F-C1, F-C2, F-B1, F-B2, F-B3 (B3+A1)

Campo de aplicación

- Objeto de evaluación: Producto o sistema a evaluar. Patrocinador, normalmente un fabricante.

- Objeto de seguridad: Clase de funcionalidad, normalmente.
- 7 niveles de evalucion de E0 a E6: confianza creciente en la corrección

Funcionalidades de seguridad

Identificación y autentificación, control de acceso, responsabilidad, auditoria, reutilización de objetos, precisión en los datos, fiabilidad del servicio.

Intercambio de datos basado en la arquitectura de seguridad de OSI:

-autenticación, control de acceso, confidencialidad e integridad de datos, no repudio

Evaluación de aseguramiento desde el punto de vista de la eficacia:

- confianza en la efectividad
- la evaluación de efectividad establece si las funciones y mecanismos ejecutores de la seguridad satisfarán los objetivos de seguridad establecidos.

Evaluación de aseguramiento desde el punto de vista de la conformidad:

- confianza en la corrección
- la evaluación de corrección se orienta a conocer si las funciones y mecanismos ejecutores de la seguridad están correctamente implementados

Resultados de la evaluación y glosario y referencias

3.3.2.3 Niveles de evaluación ITSEC

- **EO:** representa un aseguramiento inadecuado, no se emite certificado
- **E1:** a este nivel deberán existir una meta de seguridad y una descripción informal del diseño arquitectónico de la TOE
- **E2:** además de los requisitos correspondientes al nivel 1, deberá existir una descripción informal del diseño detallado. deberán evaluarse las pruebas de la realización de ensayos funcionales, deberá existir un sistema de control de la configuración y un procedimiento de distribución aprobado.
- **E3:** Además de los requisitos correspondientes al nivel 2, deberán evaluarse el código fuente y/o los esquemas del hardware correspondientes a los mecanismos de seguridad. Deberán evaluarse las pruebas de la realización de ensayos de estos mecanismos.
- **E4:** Además de los requisitos correspondientes al nivel 3, deberá existir un modelo normal subyacente de política de seguridad que soporte la meta de seguridad. Deberá especificarse en estilo semiformal las funciones dedicadas a la seguridad, el diseño detallado.
- **E5:** Además de los requisitos correspondientes al nivel 4, deberá existir una estrecha correspondencia entre el diseño detallado y el código fuente y/o los esquemas de hardware.
- **E6:** Además de los requisitos correspondientes al nivel 5, deberán especificarse en estilo formal las funciones dedicadas a la seguridad y el diseño arquitectónico, de forma coherente con el modelo formal subyacente de la política de seguridad especificado.

3.3.2.4 10 clases de funcionalidad de seguridad

- **F-C1:** Proporciona control de acceso discrecional.

- **F-C2:** Proporciona un control de acceso discrecional mas granularizado que clase C1, imputando directamente las acciones a los usuarios mediante procedimientos de identificación, auditoria de sucesos relevantes para la seguridad y el aislamiento de recursos.

- **F-B1:** Además de control de acceso discrecional, introduce funciones para mantener etiquetas de sensibilidad y se sirve de ellas para imponer un conjunto de normas obligatorias de control de acceso a todos los sujetos y objetos de almacenamiento que están bajo su control.

- **F-B2:** amplia el control obligatorio de acceso a todos los sujetos y objetos y refuerza los requisitos de autentificación de la clase B1

- **F-B3**: además de las funciones de la clase B2, proporciona funciones de soporte a roles diferenciados de administración de seguridad y la auditoria se amplia para señalar los sucesos relevantes para la seguridad.

- **F-IN**: Dirigida a sistemas con requisitos de alta integración para datos y programas. Estos requisitos podrán ser necesarios en las **bases de datos..**

- **F-AV**: Establece requisitos elevados para la disponibilidad de un sistema completo o de funciones especiales del sistema. Dichos requisitos son importantes para sistemas que controlen **Procesos de fabricación**.

- **F-DI**: Establece requisitos elevados relativos a la protección de la integridad de los datos durante el intercambio de los mismos.

- **F-DC**: Dirigida a los sistemas con elevadas demandas relativas a la confidencialidad de los datos durante el intercambio de los mismos. Un ejemplo para esta clase es el **dispositivo criptográfico**.

- **F-DX**: Dirigida a redes con elevadas demandas de confidencialidad e integridad de la información intercambiada. Este es el caso, por ejemplo, cuando debe intercambiarse información sensible a través de **redes inseguras**

Es evidente que la situación de mantener criterios de evaluación diferentes en Europa y Estados Unidos no es deseable para ninguno de los actores que participan en el proceso, especialmente para los fabricantes que tendrán que llevar a cabo evaluaciones diferentes contra diferentes criterios y esquemas para un determinado producto. Esto aumenta innecesariamente el coste de los productos sin ninguna mejora de las características de seguridad.

Por ello, en 1993 se decidió iniciar un esfuerzo para armonizar ITSEC y los Criterios Federales con el objetivo de producir un conjunto de criterios unificados para Europa y Norteamérica compatible con las prácticas existentes en ambas regiones en 1994.

La armonización de los criterios de evaluación es el primer paso para alcanzar el reconocimiento mutuo de certificados. Necesita que vaya acompañada de acuerdos sobre la metodología de evaluación, los esquemas de evaluación y las prácticas de certificación y acreditación.

Internacionales

3.3.3 BS7799 /ISO 17799

3.3.3.1 Introducción

BS 7799 es una norma que presenta los requisitos para un Sistema Administrativo de Seguridad de la Información. Ayudará a identificar, administrar y minimizar la gama de amenazas a las cuales está expuesta regularmente la información.

ISO 17799 y BS7799 son políticas de la seguridad y procedimientos de los estándares. El estándar era conocido inicialmente como BS llamado estándar británico 7799, desarrollado por la institución británica de los estándares. Más adelante, se convirtió en el estándar del IEC 17799 de la ISO cuando fue adoptado por el comité técnico del IEC de la ISO para el uso internacional.

Llaman IEC JTC 1 de la ISO y es actualmente responsable tal comité de toda la información con respecto a estándares de la tecnología, y el BS7799 se refiere específicamente al estándar de la gerencia de la seguridad de la información aprobado formalmente durante el año 2000. Este estándar define un sistema de prácticas de gerencia recomendadas de la seguridad de la información, aunque es probablemente mejor decir que el estándar es un sistema de recomendaciones, pues el IEC de la ISO recomienda que consideras cada sugerencia como intentas mejorar tu programa de la seguridad de la información, y no ver cada sugerencia como obligación inflexible de seguir.

Dependiendo de las necesidades de la seguridad de la información se puede aceptar o no aceptar los estándares BS7799. Así pues, si una recomendación particular ayuda a tratar cualquier materia de seguridad importante entonces aceptarla, si no, no hacen caso de

ella. ISO17799 y BS7799 incluyen un acercamiento abierto la mayor parte de a las ediciones comunes de la información relacionadas con los archivos electrónicos, los ficheros de datos y los archivos del software, y los documentos de papel. La información se relacionó con las notas escritas mano, materiales impresos y las fotografías, las grabaciones, las grabaciones video y las grabaciones audio, comunicaciones generales incluyendo conversaciones, conversaciones de teléfono, conversaciones de teléfono de la célula y conversaciones cara a cara, así como mensajes tales como mensajes del email, envían por telefax los mensajes, mensajes inmediatos, mensajes video, mensajes físicos, entre muchos otros artículos se consideran como definición del término "información".

Puesto que la información tiene valor y es por lo tanto un activo, necesita ser justa protegido como cualquier otro activo corporativo. La información se debe proteger apenas como la infraestructura que apoya esta información, incluyendo todas las redes, sistemas, y funciones que permitan que una organización maneje y controle sus activos de la información. BS7799 explica lo que se puede hacer para proteger los activos de la información de una organización.

Hoy, las organizaciones se hacen frente con una amplia gama de las amenazas de la seguridad, de la falta de equipo a los errores humanos, fraude, vandalismo, hurto, sabotaje, inundación, fuego, y el terrorismo uniforme en muchos países, que es manera la información necesita ser protegido. BS7799 sugiere centrarse tu atención en tres puntos principales para garantizar tu seguridad de la información, que son integridad, secreto y disponibilidad. La integridad refiere a la necesidad de proteger lo completo y la exactitud de la información así como los métodos usados para procesarla. Confidencial refiere al aseguramiento que la información se puede alcanzar solamente por la gente que tiene la autorización de hacer tan. Y la disponibilidad refiere a la garantía que las que se han autorizado para utilizar la información tienen acceso a ella y a todos los activos asociados cuando están necesitadas.

Para identificar los riesgos y necesidades de la seguridad de la información, se puede necesitar realizar un gravamen de riesgo. La mejor manera de determinar verdad esta

información es estudiar cualquier requisito legal así como la determinación de cuáles son los propios requisitos desarrollar o mejorar el propio programa de la seguridad de la información. B17799 intenta simplemente ayudar a los que investiguen mejoren sus requisitos de la seguridad de la información para la seguridad total.

ISO/IEC 17799 aplica invariablemente a organizaciones pequeñas, medianas y multinacionales. ISO/IEC 17799 comprende de cláusulas enfocadas a prácticas y métodos fundamentales de seguridad contemporánea contemplando avances tecnológicos.

ISO/IEC 27001 Especifica los requisitos para implantar, operar, vigilar, mantener, evaluar un sistema de seguridad informática explícitamente. Sobre ISO/IEC 27001 permite auditar un sistema bajo lineamientos ISO/IEC 17799 para certificar ISMS (véase también ISMSA, Organismo Internacional BRS).

La norma ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo.

La aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información.

Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización debido a que el proceso mismo de su elaboración integra mecanismos de control y por último, la certificación permite a las organizaciones demostrar el estado de la seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS7799.

3.3.3.2 Antecedentes

Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas,

privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El estándar de seguridad de la información ISO 17799, descendiente del BS 7799 – Information Security Management Standard – de la BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

- **Parte 1. Código de prácticas.**
- **Parte 2. Especificaciones del sistema de administración de seguridad de la información.**

Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 Part 1: Code of Practice).

La norma relacionada BS7799-2, es una guía de auditoria del Sistema de Gestión de Seguridad de la Información 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. Se puede aplicar el Sistema de Gestión de Seguridad de la Información de una organización a actividades separadas con las dos distintas normas.

3.3.3.3 Los controles del ISO 17799

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como Statement of Applicability, que es la definición de los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

A continuación, se describirán cada una de las diez áreas de seguridad con el objeto de esclarecer los objetivos de estos controles.

Políticas de seguridad. El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad. El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información.

Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

1) **Infraestructura de seguridad de la información:** Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización, a fin de aprobar la política de seguridad de la información,

asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización.

2) **Seguridad frente al acceso por parte de terceros:** Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

3) **Tercerización:** Mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue delegada a otra organización.

Clasificación y control de activos. El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

1) **Responsabilidad por rendición de cuentas de los activos :** Mantener una adecuada protección de los activos de la organización.

2) **Clasificación de la información:** Garantizar que los recursos de información reciban un apropiado nivel de protección.

Seguridad del personal. Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

1) Seguridad en la definición de puestos de trabajo y la asignación de recursos: Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

2) **Capacitación del usuario:** Garantizar que los usuarios conocen las amenazas y sus responsabilidades en materia de seguridad de la información en el transcurso de sus tareas normales.

3) **Respuesta a incidentes y anomalías en materia de seguridad:** Minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos.

Seguridad física y de entorno. Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

1) **Áreas seguras:** Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

2) **Seguridad del equipamiento:** Impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.

3) **Controles generales:** Impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma.

Comunicaciones y administración de operaciones. Integrar 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.

Control de acceso. Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

Desarrollo de sistemas y mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

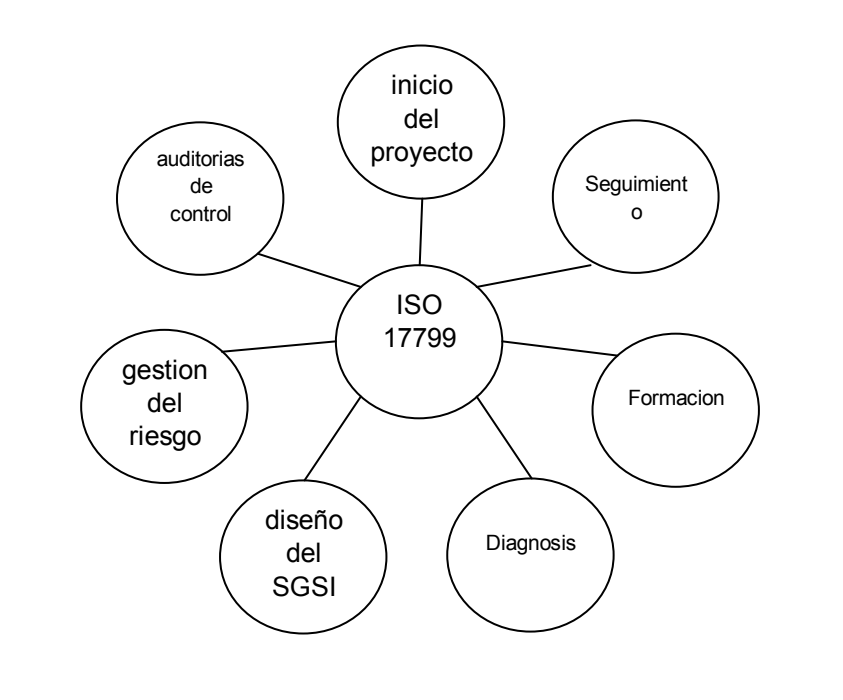
Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

Requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

3.3.3.4 Implementación de ISO 17999

Los sistemas de Gestión de la Seguridad de la Información según ISO 17799 permiten aplicar una norma global de seguridad a su organización.



Se deben definir los requisitos primordiales: compromiso de la dirección, selección del personal que afrontará en primera instancia el proyecto y campaña de sensibilización inicial. En esta fase se procederá a la recolección inicial de datos para plantear el sistema.

Diagnosis

Con los datos recopilados, se procede a realizar una diagnosis inicial de la empresa en materia de seguridad. Se realizará un informe completo de situación basado en los diez puntos de control de la norma ISO 17799

Definición del SGSI

En la definición del sistema de gestión de la seguridad de la información (SGSI) se establece el alcance del sistema, así como sus limitaciones, una vez conocida la situación inicial de la empresa

Diseño del SGSI

En esta etapa se unifican los puntos anteriores. Se elaborarán las políticas de seguridad, el manual de seguridad, los procedimientos e instrucciones de trabajo.

Gestión del Riesgo

La gestión del riesgo es crucial en un SGSI. Comprenda qué riesgos están presentes en su organización, qué implicaciones tienen, cuál es la frecuencia de aparición y el impacto de los mismos.

La implementación de controles y la correcta aplicación de activos repercutirán en la adopción de un adecuado nivel de riesgo, compatible con el normal desenvolvimiento de la organización y el coste de las operaciones.

Formación. Recursos humanos

Los SGSI requieren la participación de los recursos humanos. Entienda las debilidades que pueden suponer en la cadena del sistema. Conozca las maneras más eficientes de implicar a los recursos humanos y evitar problemas por el desconocimiento de las medidas. En esta fase se pretende diseminar el concepto de seguridad de la información a todos los estamentos implicados, profundizando en el conocimiento que deben tener para mantener del modo más elevado los estándares de seguridad.

Seguimiento

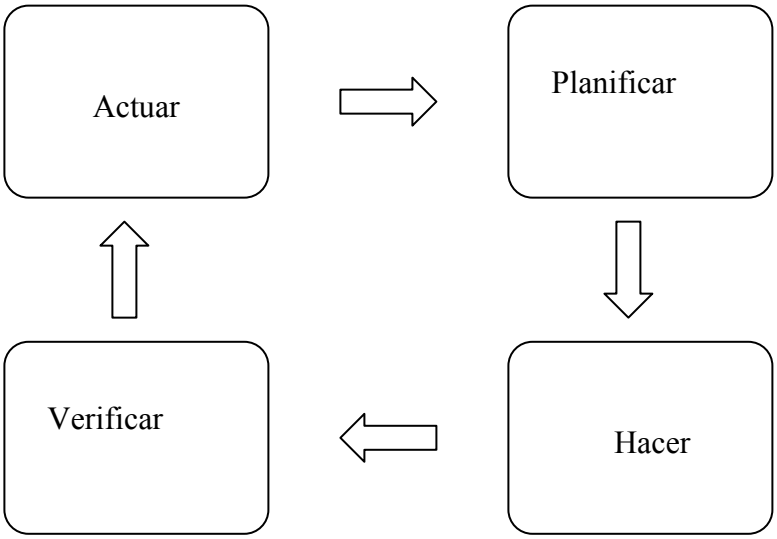
Una vez definido el sistema y puesto en marcha, tras un período de consolidación, se procede a la revisión del mismo, confrontando estos datos con la situación inicial, buscando de un modo comparativo las mejoras y los puntos donde deben emplearse acciones de mejora.

3.3.3.4.1 Porqué Implementar un ISMS / SISTEMA DE GESTION ISO17799

Algunas consideraciones generales de porqué implementarlo:

- Para poder tener una Metodológica dedicada a la seguridad de información reconocida internacionalmente
- Contar con un proceso definido para Evaluar, Implementar, Mantener y Administrar la seguridad de la información
- Diferenciarse en el mercado de otras organizaciones
- Satisfacer requerimientos de clientes, proveedores y Organismos de Contralor
- Potenciales disminuciones de costos e inversiones
- FORMALIZAR las responsabilidades operativas y LEGALES de los USUARIOS Internos y Externos de la Información
- Cumplir con disposiciones legales (por ej. Leyes de Protección de Datos, Privacidad, etc.)
- Tener una Metodología para poder ADMINISTRAR los RIESGOS

SGSI SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION esta basado en el Modelo utilizado por las NORMAS ISO en general:



3.3.3.4.2 Principales PASOS a seguir en la IMPLEMENTACION del SGSI

Implementación del SGSI en 12 PASOS:

Para un entendimiento PRACTICO del Proceso de IMPLEMENTACION del SGSI, se definen a continuación las principales TAREAS a incluir en el PLAN de ACCION son:

1) Definir el alcance del SGSI desde el punto de vista de las características de la actividad, la organización, su ubicación, sus activos y su tecnología

2) Definir una Política GENERAL del SGSI

3) Definir una METODOLOGIA para la CLASIFICACION de los RIESGOS

4) Identificar y Valorar los riesgos

5) Identificar y definir ALTERNATIVAS para el tratamiento de riesgos:

- Aplicar controles
- Aceptar los riesgos
- Evitar riesgos
- Transferir los riesgos asociados de las actividades a otras partes (ejemplo a Compañías de Seguros)

6) Seleccionar **objetivos de control** y controles específicos a IMPLMENTAR

El detalle de los controles se incluye en la Sección Dominios de ISO 17799.

Cualquier EXCLUSION de controles que se considera como necesaria para satisfacer el criterio de aceptación de riesgo, se debe justificar y se debe proporcionar la evidencia. Cuando se realizan exclusiones, no se podrá alegar conformidad con esta norma a menos que dichas exclusiones no afecten la capacidad de la organización, y/o su responsabilidad para proveer seguridad de información cumpliendo con los requisitos de seguridad determinados por la evaluación de riesgo y los requisitos regulatorios aplicables.

7) Preparar una DDA Declaración de Aplicabilidad (qué CONTROLES se van a IMPLEMENTAR)

8) Obtener la aprobación de la Dirección de:

- DDA Declaración de Aplicabilidad

- Riesgos Residuales no cubiertos

9) Formular un plan CONCRETO y DETALLADO para:

- Tratamiento de los riesgos
- Controles a Implementar
- Programas de entrenamiento y concientizacion de usuarios
- Gestionar el SGSI
- Procesos de detección y respuesta a los incidentes de seguridad

10) Implementar los CONTROLES

- Controles en los Procesos de Usuarios
- Controles Automáticos en las Tecnologías
- Documentación Respaldatoria
- Registros Respaldatorios

11) Realizar Revisiones Periódicas (Auditoría Interna y la Dirección):

- controles implementados
- nuevos riesgos
- riesgos residuales

12) Implementar las mejoras identificadas en el SGSI

3.3.3.4.3 Requisitos FUNDAMENTALES de la Documentación SOPORTE en un SGSI

Es necesario también tener en cuenta que más allá de la implementación, es necesario el MANTENIMIENTO ACTUALIZADO Y PROTEGIDO de la Documentación Respaldatoria del SGSI, para lo cual hay que establecer:

- Documentación mínima de respaldo
- Procedimiento de Gestión de dicha documentación

Documentación MINIMA del SGSI:

a) Declaraciones documentadas de la política de seguridad y los objetivos de control

b) El alcance y los procedimientos y controles de apoyo

c) El informe de evaluación de riesgos

d) El plan de tratamiento de riesgo

e) Los procedimientos documentados necesarios para la planificación, la operación y el control del SGSI

f) Los registros requeridos:Los registros se deben establecer y mantener para proveer evidencia de conformidad con los requisitos, deben permanecer legibles, fácilmente identificables y recuperables. Algunos ejemplos: logs de los sistemas para auditorias, formularios firmados de accesos, etc.

g) La DDA Declaración de Aplicabilidad

Procedimiento de GESTION de la Documentación

Los documentos requeridos deben cumplir con los requerimientos FORMALES del ISMS para:

a) aprobar los documentos previos a su distribución
b) revisar y actualizar los documentos según la necesidad y aprobarlos nuevamente

c) asegurarse de que los cambios y las revisiones de los documentos estén identificados

d) asegurarse de que las versiones más recientes de los documentos pertinentes están disponibles en cualquier punto de uso

e) asegurarse de que los documentos se mantengan legibles y fácilmente identificables

f) asegurarse de que los documentos de origen externo estén identificados

g) asegurarse de que la distribución de documentos este controlada

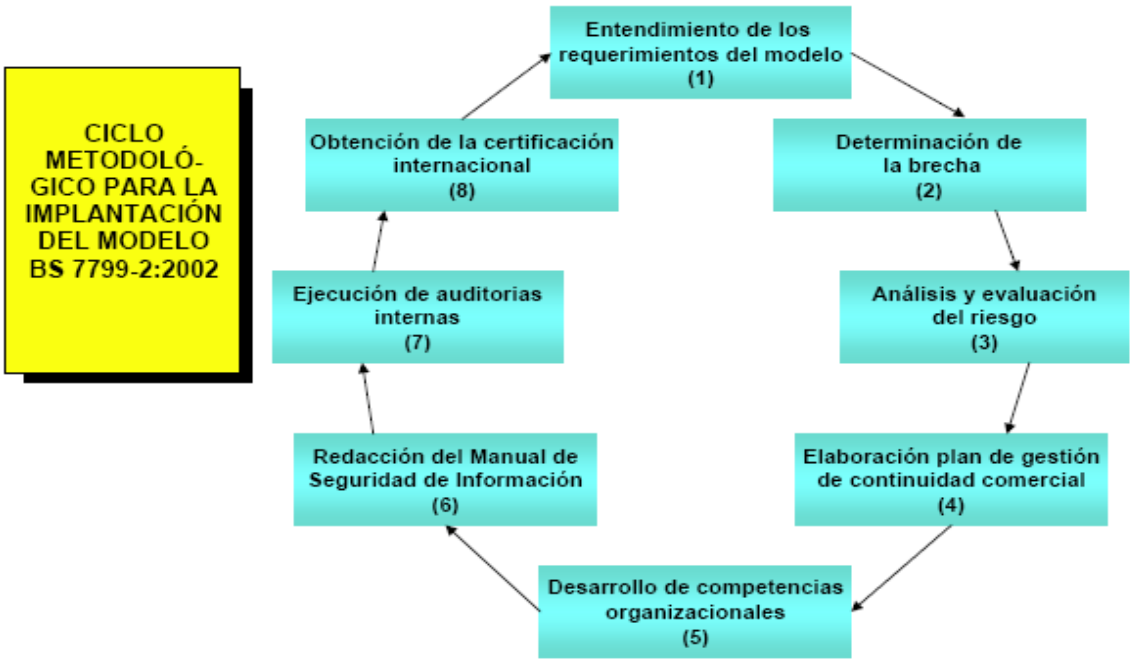
h) prevenir el uso no intencionado de documentos obsoletos

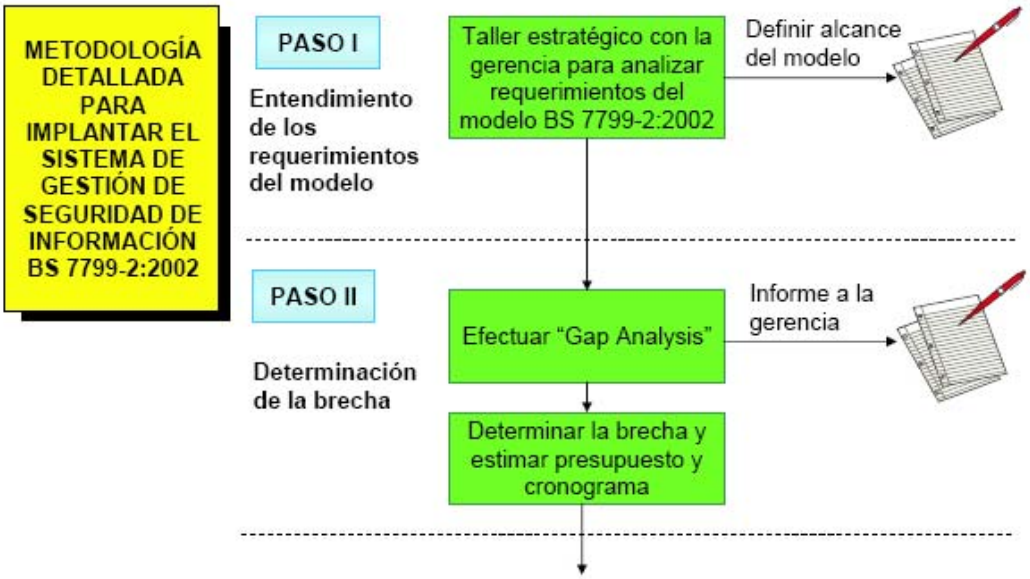
i) realizar una adecuada identificación si se retienen por cualquier causa

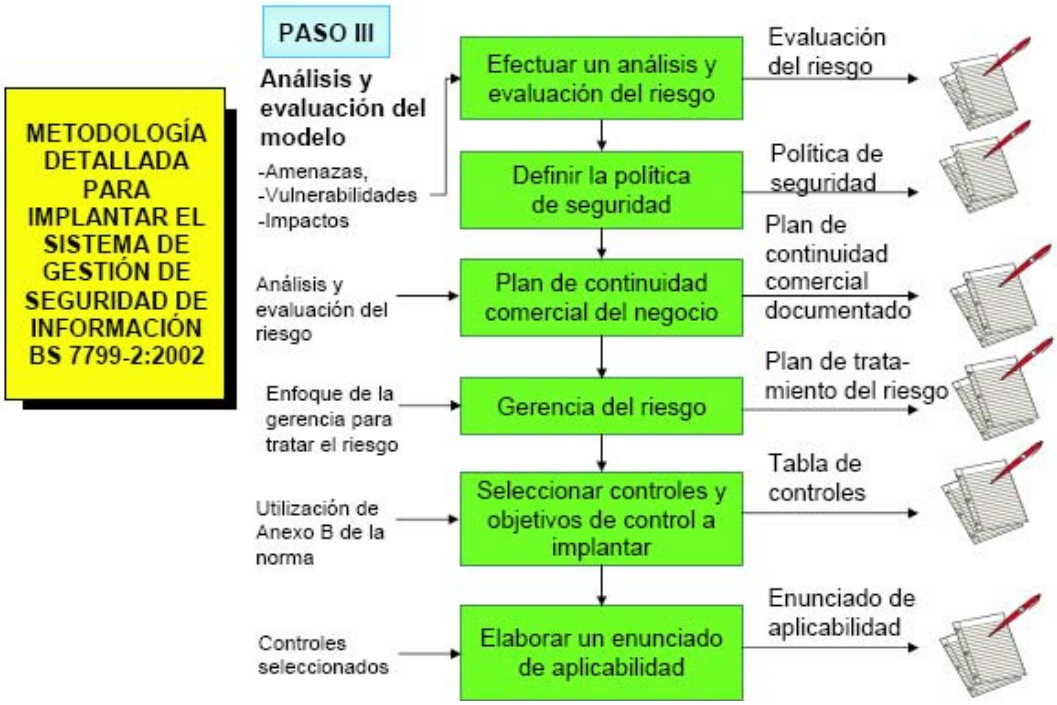
NOTA: existen Software que ayudan al mantenimiento de esta Gestión Documental disponibles en el mercado.

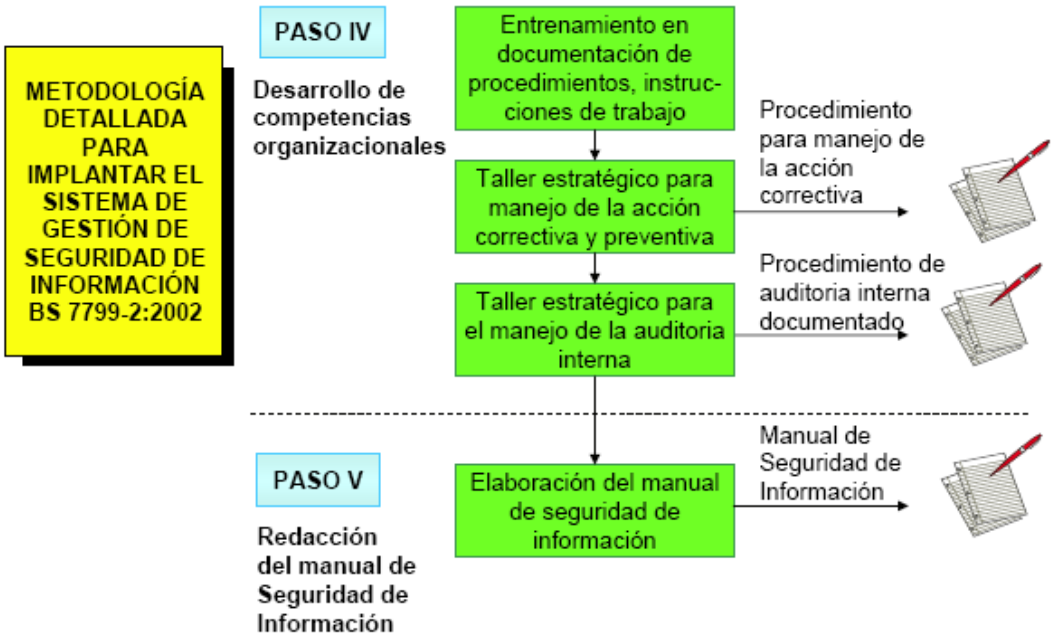
3.3.3.5 Metodología para implementar BS 7799

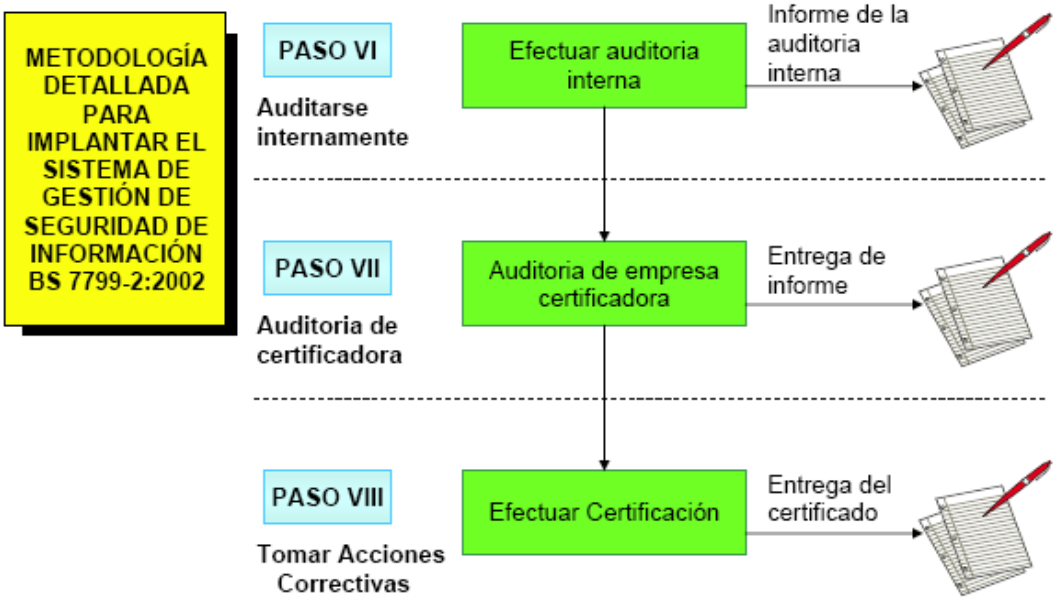
La Metodología para implantar el BS 7799 en las Organizaciones, esta compuesta de ocho fases. La idea básica consiste en efectuarle a la empresa una transferencia tecnológica para que de manera independiente la organización implante el modelo.




METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BS 7799-2:2002
PASO I
Entendimiento de los requerimientos del modelo
Taller estratégico con la gerencia para analizar requerimientos del modelo BS 7799-2:2002
Definir alcance del modelo
PASO II
Determinación de la brecha
Efectuar "Gap Analysis"
Informe a la gerencia
Determinar la brecha y estimar presupuesto y cronograma


METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BS 7799-2:2002
PASO III
Análisis y evaluación del modelo
-Amenazas,
-Vulnerabilidades
-Impactos
Efectuar un análisis y evaluación del riesgo
Evaluación del riesgo
Definir la política de seguridad
Política de seguridad
Análisis y evaluación del riesgo
Plan de continuidad comercial del negocio
Plan de continuidad comercial documentado
Enfoque de la gerencia para tratar el riesgo
Gerencia del riesgo
Plan de trata-miento del riesgo
Utilización de Anexo B de la norma
Seleccionar controles y objetivos de control a implantar
Tabla de controles
Controles seleccionados
Elaborar un enunciado de aplicabilidad
Enunciado de aplicabilidad


METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BS 7799-2:2002
PASO IV
Desarrollo de competencias organizacionales
Entrenamiento en documentación de procedimientos, instruc-ciones de trabajo
Taller estratégico para manejo de la acción correctiva y preventiva
Taller estratégico para el manejo de la auditoria interna
Procedimiento para manejo de la acción correctiva
Procedimiento de auditoria interna documentado
PASO V
Redacción del manual de Seguridad de Información
Elaboración del manual de seguridad de información
Manual de Seguridad de Información


METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BS 7799-2:2002
PASO VI
Auditarse internamente
Efectuar auditoria interna
Informe de la auditoria interna
PASO VII
Auditoria de certificadora
Auditoria de empresa certificadora
Entrega de informe
PASO VIII
Tomar Acciones Correctivas
Efectuar Certificación
Entrega del certificado

3.3.3.6 La certificación según ISO17799 o según BS7799

Tal como se comentó anteriormente, la Norma ISO 17799 está basado en el estándar británico BS7799, que tiene 2 partes:

BS7799-1 NORMALIZACION (Desarrollo de las Mejores Prácticas)

Convertido a ISO/IEC17799:2000

BS7799-2 IMPLEMENTACION SGSI / CERTIFICACION (Procesos de Auditoría para la Implementación)

En conclusión: las Organizaciones implementan de acuerdo a ISO17799-1 pero las Empresas Certificadoras utilizan el BS7799-2 para hacer los Informes de Certificación

3.3.3.7 Gestión de la Seguridad ITIL e ISO 17799

La seguridad es el asunto principal al que se enfrentan las empresas para entender los beneficios del comercio electrónico. Las empresas deben asegurarse que sus valiosos recursos y la propiedad intelectual están protegidos, y que los clientes se sienten seguros al realizar negocios.

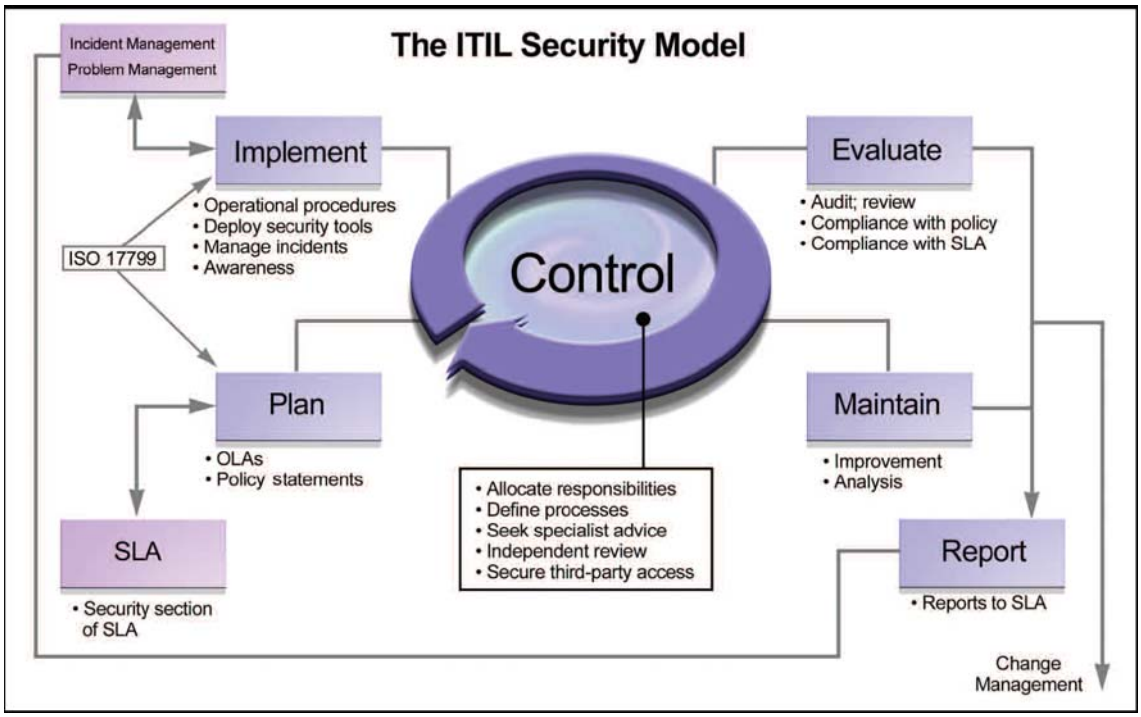
La ISO 17799 es una norma global basada en la norma británica BS7799 que define las mejores prácticas para la gestión de la seguridad de la información. Consta de las siguientes dos partes:

1. Define un conjunto de objetivos principales e identifica un conjunto de controles de seguridad, que son medidas que se pueden adoptar para cumplir los objetivos de la norma.

2. Especifica los controles de seguridad que se pueden utilizar, basándose en los resultados de una evaluación de gestión de riesgos, como base para una certificación formal de una empresa TI bajo la norma BS7799.

ITIL define los procesos de mejores prácticas para asegurar la infraestructura TI gestionada, que está en sí misma estrechamente relacionada con el uso de los procedimientos mejorados ISO 17799.

Modelo de seguridad ITIL

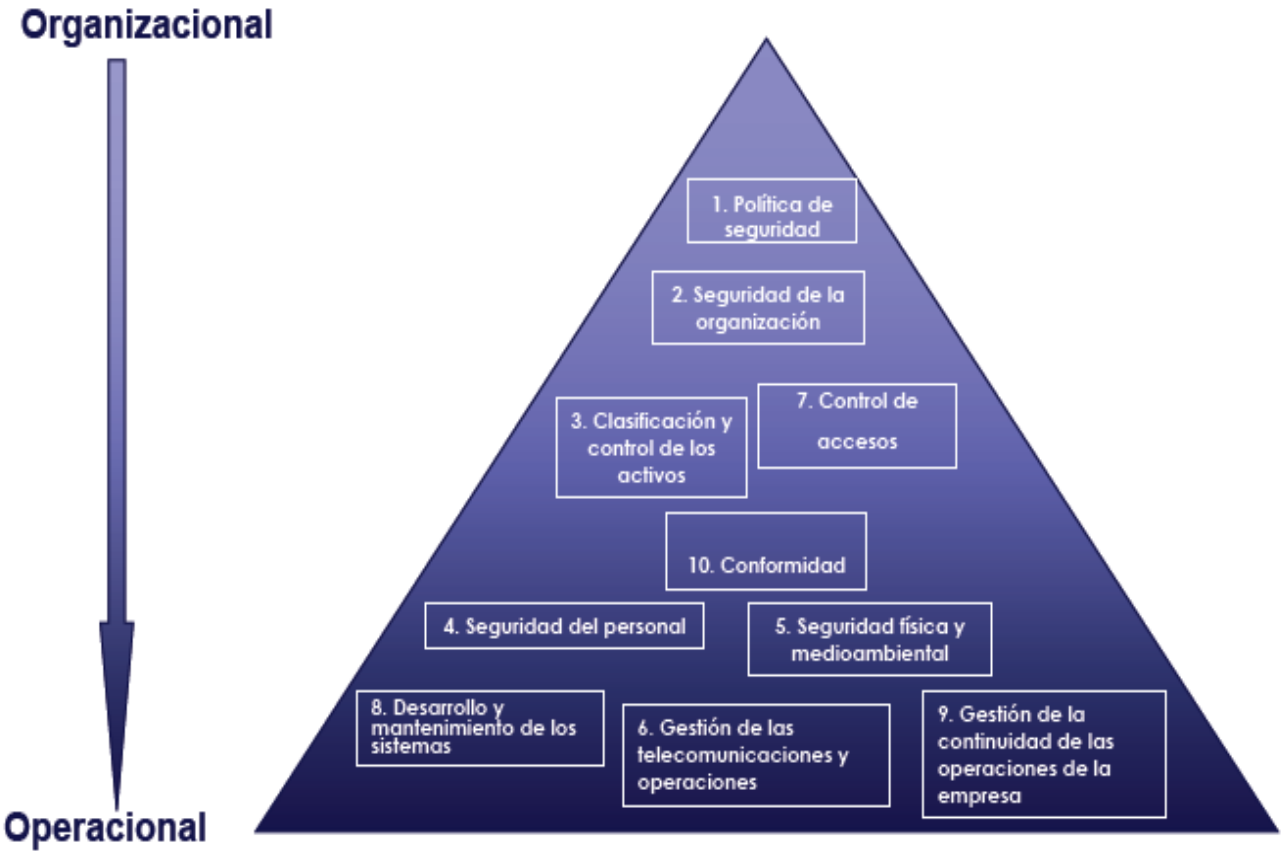


En la figura, se ilustra el flujo del proceso de seguridad ITIL.

Basado en la sección de seguridad del acuerdo de nivel de servicio (Service level agreement, SLA), el primer paso es la fase de planificación que depende de una evaluación de riesgos empresariales para comprender las amenazas y vulnerabilidades. Este proceso se basa en gran medida en la norma ISO 17799, y tiene como resultado la selección de medidas de seguridad apropiadas, que se conocen como controles. La fase de implementación es en la que se implementan estos controles, utilizando los procesos y herramientas adecuados. El resto del proceso consiste en controlar estas herramientas y procesos para seguir evaluando y revisando la política y su relación con el cambio de las condiciones empresariales; y también para mantener la política en el nivel apropiado y obtener una seguridad coherente para la empresa, y proporcionar informes para asegurar que se cumplen los SLA.

Estructura de la norma ISO 17799

ESTRUCTURA DE LA NORMA ISO 17799 EN LA ORGANIZACION



COMPLEMENTARIDAD DE LA NORMA ISO 17799 CON OTROS ESTANDARES ISO

Normas complementarias:

ISO 13335, Directrices para la Gestión de la Seguridad IT (GMITS);

ISO 15408, Criterios Comunes (CC) para la Evaluación de la Seguridad IT;

ISO 21827, Madurez de Sistemas de Seguridad.

3.3.4 COBIT

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). –COBIT es la herramienta innovadora para el gobierno de TI (Governance. Término aplicado para definir un control total)

COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicable y aceptado" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de COBIT ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

Se determinó que las mejoras a los objetivos de control originales debería consistir en:

- el desarrollo de un marco referencial para control en TI como fundamento para los objetivos de control en TI y como una guía para la investigación consistente en auditoría y control de TI;

- una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho; y

- una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en TI y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.) y

- una revisión crítica y actualización de las guías actuales para desarrollo de auditorías de sistemas de información.

.

3.3.4.1 El Marco Referencial de COBIT

LA NECESIDAD DE CONTROL EN TECNOLOGIA DE INFORMACION En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un Marco Referencial para la seguridad y el control de tecnología de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticalidad emerge de:

- la creciente dependencia en información y en los sistemas que proporcionan dicha información

- la creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información (Information warfare)

- la escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y

- el potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos Mainframe. Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

La administración debe decidir la inversión razonable en seguridad y control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración necesita un Marco Referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado.

Existe una creciente necesidad entre los USUARIOS en cuanto a la seguridad en los servicios TI, a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados.

Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general a ser establecida como primer paso.

Un enfoque hacia los requerimientos de negocio en cuanto a controles para tecnología de información y la aplicación de nuevos modelos de control y estándares internacionales relacionados, hicieron evolucionar los Objetivos de Control y pasar de una herramienta de auditoría, a COBIT, que es una herramienta para la administración. COBIT es, por lo tanto, la herramienta innovadora para el gobierno de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con TI.

Por lo tanto, el objetivo principal del proyecto COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es el desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva COSO, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos. Posteriormente, los objetivos de control fueron desarrollados a partir de la perspectiva de los objetivos de auditoría (certificación de información financiera, certificación de medidas de control interno, eficiencia y efectividad, etc.)

3.3.4.2 Orientación a objetivos de negocio

Los Objetivos de Control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoria. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Se proporcionan consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control. El Marco Referencial fue mostrado a la industria de TI y a los profesionales dedicados a la auditoria para abrir la posibilidad a revisiones, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

Existen dos clases distintas de modelos de control disponibles actualmente, aquéllos de la clase del "modelo de control de negocios" (por ejemplo COSO) y los "modelos más enfocados a TI" (por ejemplo, DTI). *COBIT* intenta cubrir la brecha que existe entre los dos. Debido a esto, COBIT se posiciona como una herramienta más completa para la Administración y para operar a un nivel superior que los estándares de tecnología para la administración de sistemas de información. **Por lo tanto, COBIT es el modelo para el gobierno de TI.**

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los

procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

Requerimientos de negocio

↗ ↘

Procesos de TI ← **Recursos de TI**

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como *requerimientos de negocio para la información*. Al establecer la lista de requerimientos, *COBIT* combina los principios contenidos en los modelos referenciales existentes y conocidos:

Requerimientos de calidad	Calidad Costo Entrega (de servicio)
Requerimientos Fiduciarios (COSO)	Efectividad & eficiencia de operaciones Confiabilidad de la información Cumplimiento de las leyes & regulaciones
Requerimientos de Seguridad	Confidencialidad Integridad Disponibilidad

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (no fallas, confiable, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo,

atractivo, "ver y sentir –*look and feel*–", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la Calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el Costo es también considerado que queda cubierto por Eficiencia.

Para los requerimientos fiduciarios, COBIT no intentó reinventar le rueda –se utilizaron las definiciones de COSO para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones–. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información –no solo información financiera.

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, fue descubierto que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas.

A continuación se muestran las definiciones de trabajo de COBIT:

- **Efectividad** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna,correcta, consistente y de manera utilizable.

- **Eficiencia** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

- **Confidencialidad** Se refiere a la protección de información sensible contra divulgación no autorizada.

- **Integridad** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- **Disponibilidad** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

- **Cumplimiento** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

- **Confiabilidad** de la información. Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de TI identificados en COBIT pueden identificarse/definirse como se muestra a continuación:

- **Datos** Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- **Aplicaciones** Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

- **Tecnología** La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

- **Instalaciones** Recursos para alojar y dar soporte a los sistemas de información.

- **Personal** Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

El dinero o capital no es considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoria financiera.

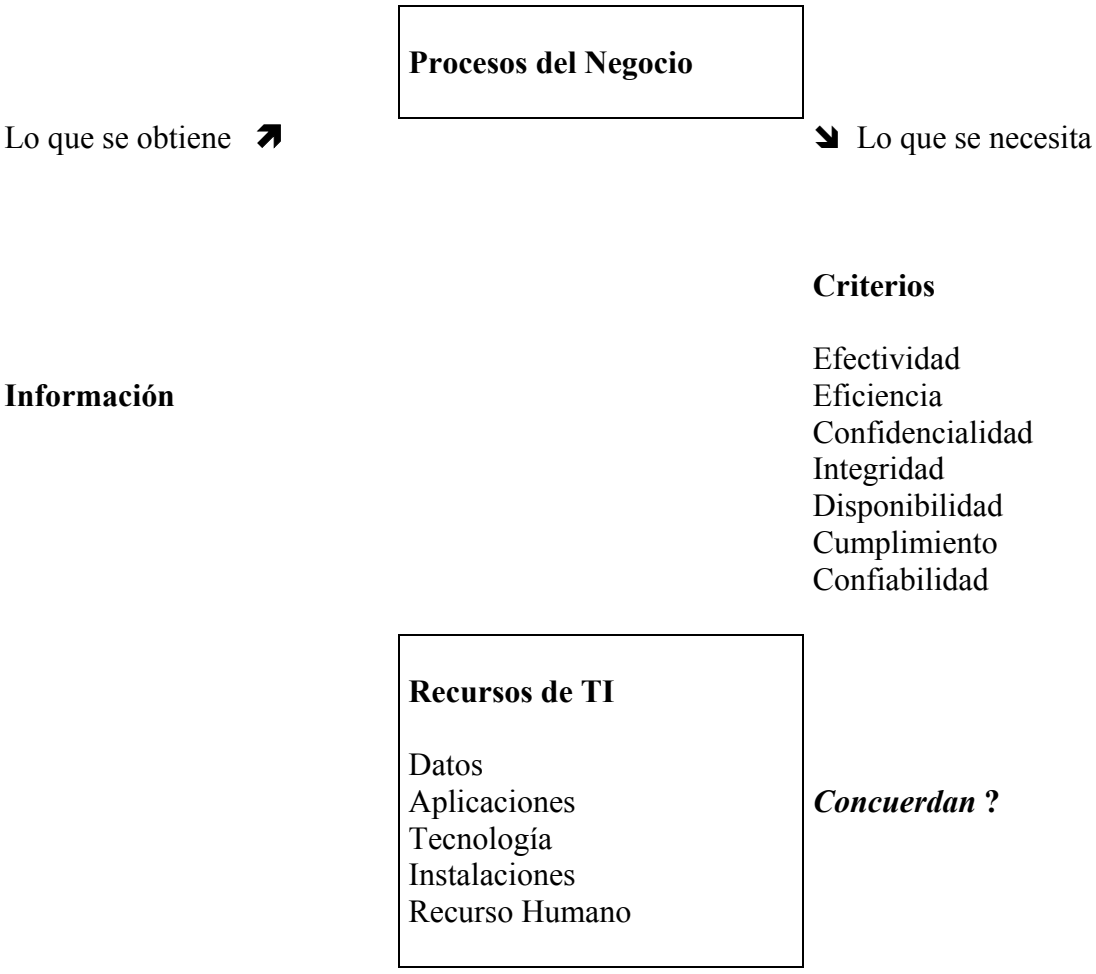
El Marco referencial no menciona, en forma específica para todos los casos, la documentación de todos los aspectos "materiales" importantes relacionados con un proceso de TI particular. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:

La información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negociio

para al información son satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos.

¿Cómo pueden entonces las empresas estar satisfechas respecto de la información obtenida presente las características que necesitan? Es aquí donde se requiere un sano marco referencial de Objetivos de Control para TI. El diagrama mostrado ilustra este concepto.

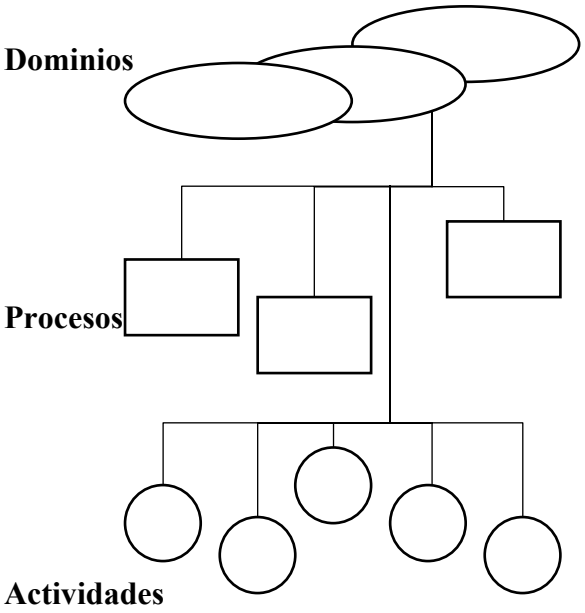


El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos.

Comenzando por la base, encontramos las actividades y las tareas necesarias para encontrar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras son consideradas más discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control).

Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.



Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización –y no la "jerga (*jargon*)" del auditor–. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo.

Las definiciones para los dominios mencionados son las siguientes:

Planeación y Organización Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición e Implementación Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y Soporte En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.*

Monitoreo Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, otros al nivel del propietario de los procesos de negocio.

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos de negocio, cubrirán algunas veces los criterios de disponibilidad, integridad y confidencialidad –en la práctica, se han convertido en requerimientos del negocio. Por ejemplo, el proceso de "identificar soluciones automatizadas" deberá ser efectivo en el cumplimiento de requerimientos de disponibilidad, integridad y confidencialidad.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial *COBIT* basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

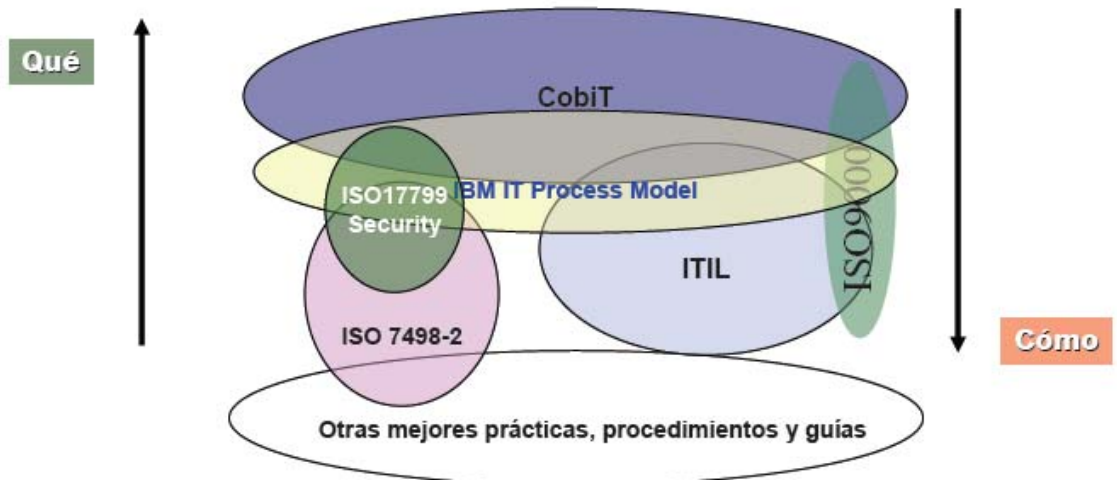
Primario es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

Secundario es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío) podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Similarmente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración (no por aquellos que simplemente toman parte en el proceso). Esta clasificación es hecha dentro el Marco Referencial de COBIT basado en el mismo proceso riguroso de información proporcionada por los investigadores, expertos y revisores, utilizando las definiciones estrictas indicadas previamente.

COBIT- ISO17799



Conclusiones

Al analizar el impacto que tienen las TIC en la vida actual, podemos concluir que la seguridad de muchos sistemas de información, es crítica ya que abarcan todo tipo de empresas, negocios, etc.

Por otra parte la integración de Internet, como herramienta cotidiana de trabajo, también ha provocado un impacto en el desarrollo de metodologías, políticas, normativas y soluciones tecnológicas para seguridad, tanto para su administración como evaluación. la razón es que fundamentalmente Internet, es una red abierta y compleja, por lo que evidentemente no se puede tener un buen sistema de seguridad, ante estas características, sin embargo, para las organizaciones actualmente es casi fundamental su uso para interrelacionarse.

La seguridad ha evolucionado tanto como las tecnologías de información , desde el "libro naranja", creado por el departamento de defensa de los Estados Unidos, hasta la normativa ISO 17799, es así como los estándares y normativas se han ido ajustando a los nuevos desarrollos de las TIC

No obstante, en la realidad, las organizaciones que implementan o intentan implementar prácticas encaminadas a lograr buenos niveles de seguridad se ven sobrepasadas, esto se debe fundamentalmente a las siguientes razones.

- En cuanto a la continuidad de las practicas de seguridad al interior de las organizaciones, es un punto critico, ya que la seguridad es mas que manuales, políticas, implementación de estándares, software, hardware, etc. tiene que ver mucho con las personas que colaboran y participan, a todo nivel de la

organización, por lo que si no existe una "cultura de seguridad", la continuidad no esta asegurada.

- La gran mayoría de los esfuerzos relacionados con la seguridad, aún después de llevar a cabo inversiones importantes en componentes tecnológicos y conocimiento, tienden a perder fuerza con el paso del tiempo lo que presupone un aumento del riesgo. Es evidente que al estar involucrado el factor humano, el tema se convierte en un asunto vivo y, como tal, debe atenderse al interior de la organización; es decir, sostener prácticas de trabajo que garanticen la seguridad de TIC debe ser un trabajo cotidiano dentro de la organización.

- Otro tema importante, es la percepción que se tiene con respecto a la inversión en seguridad, se considera que esta inversión toma valor al momento de ocurrir algún "incidente", una gran variedad de factores cualitativos están involucrados, y su medición esta determinada por los retornos de la inversión, sin embargo el estar preparado tiene costos menores que el no estarlo.

Un sistema de seguridad, debe asegurar, la integridad, disponibilidad y confidencialidad de las TIC. Esto básicamente significa que la información, los sistemas y recursos de TIC deben ser accesibles sólo para aquellos que lo tienen permitido, deben estar disponibles siempre que se necesiten y finalmente los cambios a la información, sistemas y componentes deben realizarse de acuerdo a un procedimiento específico y autorizado. Estos factores deben ser ponderados de acuerdo a cada organización, sus necesidades y requerimientos.

El uso de estándares debe ser determinado, por ende, por cada organización realizando previamente un análisis costo- beneficioso de su implementación.

Caso chileno

En nuestro país en los últimos años a cobrado una gran relevancia el tema de la seguridad de la información con tecnologías de información.

Esto, producto de la gran apertura de nuestro país y empresas a nuevos mercados. La importancia de contar con estándares ha sido vital para este proceso. Tanto para las empresas que se han abierto al comercio virtual, como para empresas que se ven afectadas por nuevas leyes internacionales como SOX.

Principalmente lo que se ha hecho en nuestro país, tiene que ver solo con códigos de buenas practicas, como por ejemplo preparar a los ejecutivos con BS7799, en ese ámbito, etc. que ya ha sido homologada en chile, pero no existe ninguna normativa legal al respecto sobre seguridad de la información, solo recientemente la "cámara de comercio de santiago" edito un "código de buenas practicas"(anexo 1), pero la legislación aun esta lejos.

Hoy en día no es necesario argumentar en defensa de la utilización de Tecnologías de Información (TI), en beneficio de una gestión más productiva y costo-efectiva por parte de las empresas. Los conceptos de seguridad también han evolucionado en forma significativa, adaptándose a la nueva tecnología y formas de operación de los sistemas modernos. Así, han aparecido múltiples herramientas tecnológicas y metodologías que prometen solucionar el problema de la seguridad de la información de las organizaciones. Sin embargo, los avances en resultados concretos son en realidad, magros. Las expectativas no están siendo satisfechas y la gran mayoría de las organizaciones, tanto públicas como privadas, enfrentan serios problemas y pérdidas asociadas al indebido y/o insuficiente resguardo de la confidencialidad, integridad y disponibilidad de la información crítica para sus actividades. Revisemos los principales

factores que inciden en la determinación de las medidas de seguridad para resguardar los activos de información de cualquier organización:

- Nivel de dependencia de las TI para el logro de la "misión": indudablemente, mientras mayor sea la dependencia de las TI, mayor será el grado de exposición a los riesgos inherentes a la utilización de tecnologías, todavía altamente propensas a fallas que vulneran la seguridad.

- Sensibilidad al riesgo: las organizaciones pueden tener distinta sensibilidad al riesgo, la que depende fundamentalmente del impacto percibido ante la eventualidad de la materialización de alguna de las amenazas identificadas (o no).

- Imposiciones derivadas del contexto legal, contractual y/o reglamentario: algunas empresas están obligadas por ley, contrato o reglamentos de organizaciones a las que pertenezcan a cumplir con ciertas condiciones de seguridad. En estos casos no queda al criterio de la empresa y deberá implementar los controles establecidos.

Todo lo anterior debiera enmarcarse en un esfuerzo corporativo cohesionado y basado en las mejores prácticas de seguridad de la información. Además de las buenas prácticas, es necesario contar con un marco legal que imponga la aplicación de medidas de seguridad para proteger la privacidad de los ciudadanos y la información sensible de sus instituciones fundamentales y estratégicas. Por supuesto, este marco legal también debiera imponer las sanciones para quienes no cumplan las medidas de seguridad que les correspondan y para aquellos que se involucren en actividades tendientes a violar la privacidad de los ciudadanos y/o acceder sin autorización a información que se haya definido como sensible para el país.

Sin embargo, a pesar de la existencia de múltiples estándares relacionados con la seguridad de productos de TI, tales como el "Common Criteria" (ISO 15408), los "Federal Information Processing Standards" (FIPS) y muchos otros que se relacionan con las recomendaciones de seguridad a nivel organizacional, tales como la ISO 17799, ISO 13335 y otros de similar aporte, no existe en el país una política o postura de lo que las instituciones públicas y privadas debieran aplicar para gestionar en forma apropiada la seguridad de sus activos de información. Tampoco contamos aún con un cuerpo de leyes que regule la aplicación de estándares para ciertos ámbitos de la industria que, por su tipo de actividad, tienen requerimientos especiales. La única excepción es la reciente Ley de Firma Digital y su Reglamento correspondiente, los que regulan las condiciones de seguridad que los proveedores de certificados digitales deben cumplir para prestar el servicio. Las leyes 19.223 (Ley de Delitos Informáticos) y 19.668 (Ley sobre protección a la vida privada de las personas) contribuyen, pero la experiencia indica que no han producido el efecto de constituir una protección legal efectiva de quienes sufren las consecuencias de un ataque cibernético.

En base a las consideraciones antes presentadas, es claro que el país requiere, a la brevedad posible, contar con la infraestructura referencial y soporte legal para proporcionar la debida protección a los recursos de información que manejan las distintas instituciones. En atención a la gran acogida y reconocimiento que ha tenido, el cuerpo referencial de buenas prácticas debiera basarse en la ISO 17799, debidamente complementada con las metodologías que lleven a terreno práctico, de acuerdo a diversas realidades de requerimientos y presupuestos, las recomendaciones de carácter de alto nivel que proporciona la ISO. La ISO 17799 tiene la bondad de ser transversal a las organizaciones, abarcando la seguridad como un problema integral y no meramente técnico, error común de muchas metodologías propietarias existentes en el mercado. Su crítica más frecuente es que no proporciona soluciones concretas para los problemas comunes en las organizaciones, sino que entrega recomendaciones de carácter genérico.

Esta característica es precisamente lo que permite su aplicabilidad a distintos ámbitos de la industria, ya que la empresa que aborde un proyecto de seguridad basado en la ISO deberá interpretar estas recomendaciones en base a su realidad de requerimientos de seguridad, sensibilidad al riesgo y capacidad presupuestaria. La certificación correspondiente acreditaría que la empresa ha analizado en forma acuciosa sus riesgos y ha resuelto implementar los controles que llevan el riesgo a un nivel aceptable. El nivel de seguridad final es variable entre una empresa y otra, dado que sus necesidades seguramente no serán iguales.

Actualmente el Instituto Nacional de Normalización (INN) se encuentra desarrollando una versión nacional de la ISO 17799 (NCH 2777) para su uso en el contexto de la Ley de Firma Digital. Esta iniciativa constituye una buena partida al esfuerzo de una política nacional de seguridad de la información, pero debiera ser aplicable en forma más amplia para que sea un aporte efectivo. Claramente, esta norma debiera incluir los mecanismos de certificación y acreditación de su cumplimiento, de manera que las empresas puedan demostrar su preocupación por la seguridad de la información.

Con respecto al cuerpo legal de soporte para la infraestructura de seguridad del país, es importante analizar los principales aspectos que esta ley (o leyes) debiera incorporar para tener la efectividad que se requiere. A continuación se plantean los "efectos deseados" que se perciben como prioritarios:

- Obligación de proteger la información privada de los clientes por parte de los proveedores de servicios, cualquiera sea su naturaleza. Esto implica que debiera definirse en forma clara las categorías de información que requieren protección y, para cada categoría, establecer los mecanismos mínimos en forma de referencia a las buenas prácticas reconocidas internacionalmente, las que pueden

estar "localizadas" en una norma como la NCH 2777 antes mencionada. Un ejemplo de una primera ley de la naturaleza que se propone, lo constituye la recientemente promulgada Ley de Firma Digital. Asimismo, se encuentra en estudio en el Congreso un proyecto de ley para actualizar y perfeccionar la ley de delitos informáticos, incorporando figuras delictivas no visualizadas anteriormente, las que son fruto de la experiencia a la fecha.

- Analogía del mundo físico al mundo digital, desde el punto de vista de lo que sea considerado como violación al derecho de privacidad. Por ejemplo, si no es aceptable que una persona que pasa por la calle pruebe las ventanas y puertas que queden a su alcance, tampoco debiera serlo que un "hacker bien intencionado" verifique el nivel de seguridad de los sistemas visibles desde Internet. Esto implica crear los argumentos para que sea posible iniciar acciones legales efectivas en contra de quienes no respeten la privacidad de las personas e instituciones, intentando penetrar sistemas de seguridad o ingresando sin autorización explícita a sitios insuficientemente protegidos.

Estos "efectos deseados" son conceptualmente fáciles y obvios. Sin embargo, dada la complejidad y dinamismo del mundo TI, la redacción de estas leyes representa una tarea larga y ardua que debiera incorporar a diversos actores del mercado, de manera de cubrir en forma completa todas las posibles aristas. Para asegurar el éxito de un esfuerzo destinado a proporcionar al país una infraestructura de seguridad que permita aprovechar al máximo las ventajas de las Tecnologías de la Información y proyectarnos como un país ejemplo para la región y el resto del mundo, debemos actuar con rapidez, altura de miras, visión futurista y desapego a las posturas individuales de los distintos actores del mercado.