UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

POSGRADO EN CIENCIA E INGENIERIA DE LA COMPUTACION

METODOLOGIA PARA LA APLICACION DE LA NORMA ISO/IEC 17799

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRA EN CIENCIAS

(COMPUTACION)

PRESENTA:

CINTIA QUEZADA REYES

DIRECTOR DE TESIS:

DR. ENRIQUE DALTABUIT GODAS

MEXICO, D. F. **2006**

"Agradece a la llama su luz, pero no olvides el pie del candil que constante y paciente la sostiene en la sombra."
Rabindranath Tagore

A mis padres Náyade Reyes y Luis Quezada
Porque su motivación, amor y confianza son mis armas principales para luchar contra todos los obstáculos. Ambos son el estímulo principal que me ha llevado a seguir superándome día con día, pues todo lo que he logrado es gracias a ustedes y por ustedes.

A mi hermana Aída Quezada
Por estar presente en todo momento, mi vida no sería la misma si no existiera alguien que me ayudara a duplicar mis alegrías y a minimizar mis angustias. Te quiero mucho.

A mis tías Ceres Reyes y Elvia Santiago
Porque la fortaleza necesaria para alcanzar mis metas se basa en su apoyo, cariño y confianza.

A Sergio Gutiérrez
Por brindarme todo el apoyo, cooperación, dedicación y cariño; por compartir tus sueños, tu vida y tu corazón. Gracias por dejarme compartir contigo mis alegrías, preocupaciones, tristezas y anhelos. Es muy importante que alguien tan especial exista en mi vida. Te amo.

A Ma. Jaquelina López
Por brindarme tu amistad tan preciada, compartir tu sabiduría, incentivarme en todo momento y apoyarme día con día, definitivamente eres parte esencial de este éxito tan anhelado.

A mis amigos Joel Aguilar, Carlos Aroche, Hugo Cedillo, Juan Carlos Farfán, Daniel Hernández, Oscar Herrera, Moisés León, Guadalupe Morales, Pablo Orozco, Carlos Saucedo, Ariadna Suárez y Carlos Torres.
Porque nuestra amistad afortunadamente no depende del espacio ni del tiempo, agradezco que siempre han creído en mí, su continuo interés me motiva a lograr los objetivos que me he planteado.

A mis compañeros
Por todo el apoyo brindado, en especial a Rogelio Maldonado, Rosa Rodríguez, Miriam Gómez y Víctor Fajardo porque hoy en día nos une una valiosa amistad.

A mis maestros
Por compartir sus conocimientos y experiencias, pues éstos son dos elementos indispensables que me han ayudado a crecer de manera profesional y como ser humano.

Al Dr. Enrique Daltabuit
Gracias por el apoyo incondicional, su valiosa cooperación, el tiempo brindado, la continua dedicación, enseñanzas, comentarios y sugerencias que fueron de suma importancia para la creación y culminación de este trabajo.

A la Universidad Nacional Autónoma de México
Por ser mi Alma Mater, es un verdadero orgullo haber recibido tantas enseñanzas de la universidad que ha sido, es y seguirá siendo la Máxima Casa de Estudios.

A Dios
Por todo lo que me ha dado en la vida.

ÍNDICE

INTRODUCCIÓN

La gestión de la seguridad de una organización puede ser - y en muchos casos es - algo infinitamente complejo, no tanto desde un punto de vista puramente técnico sino más bien desde un punto de vista de la gestión de seguridad de la organización; no se tiene más que pensar en una gran universidad o empresa con un número elevado de departamentos ò áreas, ya que si alguien que pertenece a uno de ellos abandona la organización, eliminar su acceso a un cierto sistema no implica ningún problema técnico, pero sí graves problemas a la organización. Esto se debe a que un administrador de sistemas no siempre se entera que un cierto usuario, que no trabaja directamente junto a él, abandona la empresa, otro problema es saber quién decide si al usuario se le elimina directamente o se le permite el acceso a su correo durante un mes, es entonces cuando surge la interrogante de si puede el personal del área de seguridad tomar la decisión de bloquear el acceso a alguna persona perteneciente a cierta jerarquía en la organización, como un directivo o un director de departamento, una vez que éste abandone la empresa.

Hoy en día, una entidad que trabaje con cualquier tipo de información, desde pequeñas empresas con negocios no relacionados directamente con las nuevas tecnologías hasta grandes organizaciones de ámbito internacional, está - o debería estar - preocupada por su seguridad. Y no es para menos, el número de amenazas a la información, entornos informáticos y de comunicaciones crece año tras año, es previsible que la preocupación por la seguridad vaya en aumento conforme aumente la necesidad de distribuir información a nivel nacional e internacional Hasta hace poco, se centraba sobre todo en los aspectos más técnicos de la seguridad y bastaba con convencer a algún responsable técnico que con la implantación de un firewall corporativo se acabarían todos los problemas de la organización, y por supuesto se elegía el más caro aunque después nadie supiera implantar en él una política correcta; poco después y en vista de que el firewall no era la panacea, se convencía a la dirección que lo que realmente estaba de moda eran los sistemas de detección de intrusos, y por supuesto se adquiría un producto de este tipo.

Actualmente la seguridad va más allá de lo que pueda ser un firewall, un sistema de autenticación biométrico o una red de sensores de detección de intrusos pues ya se contemplan aspectos que hasta hace poco se reservaban a entornos altamente cerrados, como bancos u organizaciones militares. Y es que se ha notado que sin un plan de continuidad del negocio en caso de catástrofe y sin una política de seguridad correctamente implantada en la

organización, no sirven de nada los controles de acceso (físicos y lógicos) a la misma. Se habla ahora de la gestión de la seguridad como algo crítico para cualquier organización, igual de importante dentro de la misma que los sistemas de calidad o las líneas de producto que desarrolla.

Algo que sin duda ha contribuido a todo esto, es el interés que han mostrado diversos organismos por crear documentos y guías cuyo contenido presente lineamientos, principios, políticas, recomendaciones y/o buenas prácticas de seguridad, entre los más reconocidos se encuentran:

1. Pautas de la OECD para la seguridad de los sistemas de información (1992).

2. Libro para desarrollar políticas de seguridad, por Michele D. Guel del instituto SANS (2001).

3. Política de uso de la computadora y la red, por el Instituto de tecnología de Georgia (2001).

4. Guía de seguridad informática, por SEDISI (2002).

5. Pautas de la OECD para la seguridad de la información en sistemas y redes (2002).

Como se observa, desde 1992 con el documento realizado por la OECD y que sirvió como base, han existido diversos y continuos esfuerzos que finalmente dan paso a la aparición de normativas y estándares de seguridad de ámbito internacional y a su aplicación efectiva, de tal forma que las empresas de varios países se preocupan por la correcta gestión de su seguridad.

Por tales motivos, la finalidad de este trabajo es la introducción de los aspectos generales del proceso para implementar la gestión de la seguridad de la información con base en el estándar detallado de seguridad ISO/IEC 17799.

A continuación se muestra cómo está conformado el trabajo y se describe brevemente el contenido de cada capítulo.

Debido a los grandes avances tecnológicos y a la continua preocupación de las empresas por lograr un buen manejo de la seguridad de su información tomando como base un estándar internacional, el *capítulo 1* describe a detalle

un panorama general de los antecedentes, desarrollo y creación del estándar *ISO 17799*.

Parte esencial de un correcto manejo de la seguridad de la información se basa en el análisis del riesgo, ya que éste permite identificar las consecuencias probables o los riesgos asociados con las vulnerabilidades, además permite realizar un juicio sobre la seguridad de la información de la organización, debido a su importancia, el *capítulo 2* describe la terminología que se emplea en un *análisis del riesgo* y los pasos que se deben seguir para llevarlo a cabo.

Una vez que se haya realizado el análisis del riesgo con el que se identifican los requerimientos de seguridad, se seleccionan e implementan los controles del estándar ISO 17799 para reducir los riesgos a un nivel aceptable. El *capítulo 3* detalla las diez *secciones del estándar* - cada una cubre una cierta área - mencionando sus objetivos y controles para una correcta implementación.

La *aplicación del estándar* se basa en el proceso mencionado en el *capítulo 4*, un ejemplo de una estructura de organización de la seguridad que resulta de la aplicación de dicho proceso también puede observarse en este capítulo.

Finalmente, en las conclusiones se mencionan los puntos a resaltar tras la elaboración del presente trabajo, ya que el tema que se trata forzosamente debe ser de gran importancia para todos aquéllos que se encuentran involucrados en el manejo de la seguridad de la información y buscan un punto de referencia único e internacional para identificar los controles necesarios en la mayoría de las situaciones en que los sistemas de información se ven involucrados en la industria y el comercio.

CAPÍTULO 1

ISO 17799

1.1 Antecedentes

El funcionamiento de la seguridad para proteger la información es un aspecto importante para las actuales organizaciones. Aunque el proceso de implementación de políticas completas de seguridad puede resultar intimidante, muchas organizaciones que se enfrentan a retos cada vez mayores en materia de seguridad adoptan normas sin el proceso de certificación y lo utilizan simplemente como guía de los mejores procedimientos, sin embargo, un proceso de certificación con base en un estándar asegura a los clientes y asociados que la información distribuida o guardada en las redes empresariales se encuentra segura y que la seguridad general de la organización es confiable.

Una empresa certificada bajo un estándar internacional de seguridad de la información puede administrar ésta con eficiencia y efectividad, reduciendo vulnerabilidades y teniendo un mejor manejo de los riesgos - la organización se mantendrá actualizada en las últimas vulnerabilidades y mejores procedimientos de la seguridad mediante auditorías y revisiones externas continuas. La reducción de las vulnerabilidades significará menores transgresiones a la seguridad, lo cual generará una disminución de los fraudes, de los riesgos financieros y jurídicos, logrando así ahorro de tiempo, credibilidad en la información y la confianza de los clientes.

1.1.1 El estándar BS7799

En respuesta a la demanda industrial, un grupo dedicado a la seguridad de la información se creó en mayo de 1987 – llamado Centro Comercial de Seguridad en Cómputo del Departamento Británico de Comercio e Industria (CCSC - DTI) -, teniendo a su cargo dos tareas principales:

1. Brindar ayuda a los vendedores de productos de seguridad de tecnología de la información mediante el establecimiento de un conjunto de criterios internacionalmente reconocidos de evaluación de seguridad y un esquema asociado de evaluación y de certificación. Esto dio lugar a los Criterios de Evaluación de Seguridad de Tecnología de la Información (ITSEC), y finalmente al establecimiento del esquema ITSEC del Reino Unido.

2. Brindar ayuda a los usuarios mediante un código de buenas prácticas de seguridad. Esto dio lugar al "Código de práctica para usuarios" que fue publicado en 1989.

Éste último fue retomado y desarrollado por el Centro Nacional de Cómputo (NCC) y años más tarde por un grupo de usuarios de la industria británica para asegurar que el código fuera significativo y práctico desde el punto de vista del usuario. El resultado final se publicó por primera vez en febrero de 1993 como un documento guía del estándar británico (BS), recibiendo el nombre "PD 0003: Código de práctica para el manejo de seguridad de la información". Este trabajo fue contemplado y perfeccionado, dando lugar a la primera versión del estándar británico BS7799[1], publicándose y poniéndose finalmente en circulación en 1995 y apareciendo una versión revisada del estándar un año más tarde.

En 1998, el Instituto Británico de estándares (BSI) formó un programa para acreditar a las firmas auditoras - tanto cuerpos de certificación como auditores individuales - para que fueran capaces de auditar organizaciones que buscaban lograr la conformidad con base en el estándar BS7799. Este esquema de acreditación es conocido como C:cure, estuvo bajo la supervisión y desarrollo del departamento que inspecciona la estandarización en Tecnología de Información (TI) y telecomunicaciones llamado departamento de Entrega de Soluciones de Información para Clientes del Instituto Británico de estándares, mejor conocido como BSI/DISC, e involucraba activamente a otros organismos interesados como al Servicio de Acreditación del Reino Unido (UKAS), a la Sociedad Británica de Cómputo (BCS) y al Registro Internacional de Auditores Certificados (IRCA).

El objetivo de C:cure:

a) Proveer un nivel de confianza alto a las organizaciones y a sus socios comerciales buscando la seguridad de sus activos y recursos de Tecnología de Información.

De manera simultánea al programa para acreditar a las firmas auditoras, se formó un comité – conformado por el departamento de información BSI/DISC, en donde varias organizaciones de TI como la Agencia Central de Cómputo y Telecomunicaciones (CCTA), la Sociedad Británica de Cómputo (BCS) y compañías como Marks & Spencer y Shell se vieron envueltas en las consultas que produjeron modificaciones al estándar - que culminó con la inclusión de una segunda parte del estándar en febrero de 1998 y la actualización y circulación de la primera parte en mayo de 1999. En esta

[1] Siglas obtenidas por su nombre en inglés British Standard.

última versión se reemplazan las referencias a *Tecnología de Información* con la palabra información, también fue revisada en otras áreas para establecer de manera clara que el tema de seguridad de la información no se restringe únicamente al departamento encargado de la TI ya que es una responsabilidad corporativa. Además, la versión de 1999 fue producto de un equipo internacional de escritores de Australia, Brasil, Alemania, Irlanda, Países Bajos, Noruega, Suecia, Reino Unido y Estados Unidos que colaboraron con comentarios y revisiones.

Debido a la gran aceptación que mostró la norma en países como Australia, Sudáfrica, Nueva Zelanda, Holanda y Noruega, el gobierno del Reino Unido recomendó como parte de su "Ley de Protección a la Información de 1998" – la cual entró en vigencia a partir del 1° de marzo de 2000 - que las compañías británicas utilizaran el estándar BS7799 como método de cumplimiento de esa ley.

Los objetivos del estándar son:

a) Capacitar a una organización para que implemente de manera apropiada la seguridad de la información.

b) Proveer una guía común de mejores prácticas.

c) Facilitar el comercio entre compañías proporcionando confianza en la seguridad de la información compartida.

d) Brindar a los profesionales de tecnología de información un anteproyecto para que desarrollen políticas y procesos de seguridad empresarial.

El estándar BS7799 es un conjunto de controles[2] de seguridad y metodologías para su correcta aplicación, actualmente se compone de dos partes y existe una versión actualizada de la segunda desde el 5 de septiembre de 2002.

a) Parte 1: Código de práctica - es una guía de implementación basada en sugerencias, ya que es un conjunto de controles que incluye las

[2] Medida contra vulnerabilidades. Presentan una meta que debe ser alcanzada y lo que debe hacerse – puntos que deben ponerse en práctica - para lograrla.

buenas prácticas de administración de seguridad de la información. Esta parte es utilizada como un medio para evaluar y construir una infraestructura amplia y sólida de la seguridad de la información, incluso detalla acciones de seguridad de la información que una organización debe hacer.

b) Parte 2: Especificación - es una guía de revisión basada en requerimientos, ya que contiene las especificaciones para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento de un sistema de administración de seguridad de la información (SASI) documentado y basado en los controles y objetivos de control establecidos en la primera parte. Para certificarse bajo el estándar BS7799, las organizaciones se auditan en comparación con esta segunda parte del estándar, ya que detalla las acciones de seguridad de la información que una organización haría, sin embargo, es indispensable hacer notar que esta rigidez impide la aceptación y el soporte de manera muy general. El plan de seguridad o SASI consta de cuatro fases:

- Evaluación de riesgos: es el análisis de lo que puede suceder y el impacto que el incidente puede tener en los objetivos de la organización. Los códigos maliciosos y accesos no autorizados son ejemplos de riesgos.

- Manejo de riesgos: es el plan que la organización puede utilizar para reducir los riesgos. Los métodos utilizados en el manejo de riesgos no sólo comprenden dispositivos de seguridad de la red, sino también la seguridad física, procedimientos administrativos, planes de contingencia e iniciativas de los recursos humanos.

- Implementación de los dispositivos de seguridad: son las herramientas actuales y recursos identificados y adoptados por la organización para minimizar los riesgos.

- Instructivo de aplicabilidad: es un plan de seguridad que se requiere para la acreditación BS7799. Este instructivo contiene los controles de seguridad que la organización ha adoptado y las razones por las cuales se tomaron esas medidas. Además la organización debe listar los controles específicos de BS7799 que no se han utilizado y explicar porqué.

1.2 ¿Qué es el estándar ISO 17799?

Actualmente, la seguridad de la información se ha convertido en grandes encabezados de noticias y se ha vuelto una preocupación para los usuarios de computadoras a nivel mundial. Mientras algunas organizaciones utilizaron el estándar BS7799 como base, otras expresaron la necesidad de un estándar común, por lo que la demanda de un estándar dirigido al manejo de la seguridad de la información reconocido mundialmente bajo el amparo de un cuerpo de carácter internacional como la Organización Internacional para la Estandarización (ISO) creció.

Esta demanda condujo al rápido seguimiento de la primera parte del estándar BS7799, culminando en su primer lanzamiento realizado por la ISO en Diciembre de 2000 y teniendo como nombre ISO/IEC 17799:2000. La primera parte del estándar BS7799 fue aceptada por este organismo internacional debido a que puede ser aplicado mundialmente e invariablemente a todos los tipos de organización - pequeñas, medianas y multinacionales – y a múltiples aplicaciones. Aun cuando se buscó la adopción de la segunda parte del estándar británico por parte de la ISO, hoy en día este objetivo se ha descartado.

A pesar de la controversia ocasionada entre aquéllos que creían que los estándares deberían ser más precisos, ISO 17799 es el único estándar de alto nivel y de naturaleza conceptual[3] dedicado al manejo de la seguridad de la información en un campo gobernado generalmente por "Principios" y "Buenas prácticas". La normativa ISO 17799 contiene elementos y cláusulas enfocados a prácticas y métodos fundamentales de seguridad contemplando los avances tecnológicos. Desde su publicación surge como el estándar de seguridad de la información más reconocido a nivel mundial.

Este estándar define a la información como un activo o recurso que existe de muchas formas y que tiene valor para una cierta organización, la información puede estar impresa o escrita en un papel, almacenada electrónicamente, ser transmitida por correo o mediante medios electrónico e incluso transmitida mediante una conversación. Cualquiera que sea la forma que la información tome o los medios por los cuales sea almacenada o compartida, siempre debe estar propiamente protegida.

[3] Perteneciente o relativo al pensamiento expresado con palabras después de examinadas las circunstancias.

La meta de la seguridad de la información es proteger este recurso de manera oportuna y conveniente de un rango muy amplio de vulnerabilidades, de tal manera que se asegure la continuidad del negocio, se minimicen los daños y se maximicen las ganancias de las inversiones y las oportunidades de negocio.

Como está definido por ISO 17799, la seguridad de la información es la conservación de:

1. Confidencialidad: asegurar que la información sea accesible sólo para aquéllos que están autorizados para tener acceso.

2. Integridad: preservar la exactitud y evitar la modificación no autorizada de la información y métodos de procesamiento.

3. Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y recursos asociados cuando sean requeridos.

4. Autenticidad: asegurar la veracidad de la información.

La seguridad de la información se logra tras implementar un adecuado conjunto de controles, los cuales pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Estos controles necesitan establecerse para asegurar que los objetivos específicos de seguridad de la organización se alcancen.

El estándar ISO 17799 no es:

1. Un estándar técnico.

2. Un producto o tecnología dirigida.

3. Una metodología de evaluación del equipo o las herramientas como los Criterios Comunes/ISO 15408[4], la cual trata con requerimientos funcionales y seguros de un equipo en específico.

[4] http://www.commoncriteriaportal.org/

4. Afín con los "Principios Generalmente Aceptados de Seguridad del Sistema" (GASSP)[5], el cual es una colección de buenas prácticas de seguridad.

5. Afín a la quinta parte de "Principios para el manejo de Seguridad de Tecnología de Información" (GMITS/ ISO 13335)[6], la cual provee un marco conceptual para el manejo de la seguridad de la de tecnología de información.

Debido a que el estándar sólo cubre la selección y el manejo de los controles de seguridad de la información, es necesario considerar que estos controles deben:

1. Requerir la utilización de un nivel de seguridad del equipo de los Criterios Comunes (EAL).

2. Incorporar los Principios Generalmente Aceptados de Seguridad del Sistema.

3. Implementar conceptos de los Principios para el manejo de Seguridad de Tecnología de Información.

1.2.1 Beneficios de ISO 17799

La seguridad perfecta pueden lograrla sólo los servidores desconectados y localizados en cuartos sin puertas. La seguridad de la información siempre es un asunto de cambios que balancea los requerimientos de negocios en contraste con la tríada que incluye la confidencialidad, la integridad y la disponibilidad.

El proceso de la seguridad de la información tradicionalmente se ha basado en amplios principios y mejores prácticas, con la meta de prevenir, detectar y contener brechas o fracturas de seguridad y restaurar los datos afectados dejándolos en su estado anterior.

Es de vital importancia hacer notar que las organizaciones desean ser capaces de implementar los controles de seguridad de la información para conocer y resolver sus propios requerimientos de negocio así como un

[5] http://web.mit.edu/security/www/gassp2.html
[6] http://www.iso.org/

conjunto de controles para las relaciones de negocio que mantienen con otras organizaciones. Estas organizaciones muestran la necesidad de compartir los beneficios de la práctica común en un nivel internacional para asegurar que son capaces de proteger sus procesos y actividades de negocio para satisfacer las necesidades de éste.

Es por esto que el estándar ISO 17799 ofrece un punto de referencia para construir la seguridad de la información organizacional y un mecanismo para manejar este proceso.

Este estándar es un proceso de seguridad de la información que le asegura a las empresas los siguientes beneficios:

1. Una metodología estructurada internacionalmente reconocida.

2. Un proceso definido para evaluar, implementar, mantener y manejar la seguridad de la información.

3. Un conjunto de políticas severas, estándares, procedimientos y principios.

4. La certificación permite a las organizaciones demostrar su propio estado de seguridad de información y evaluar el de sus socios.

Para algunas organizaciones, incluso aquéllas que requieren altos grados de seguridad y confianza, la certificación ISO 17799 debe ser obligatoria, para otras, la certificación debe ser una herramienta de mercado, esto se debe a que una empresa certificada con el estándar ISO 17799 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa certificada. Además una empresa certificada tendrá en cuenta lo siguiente:

1. Mayor seguridad en la empresa.

2. Planeación y manejo de la seguridad más efectivos.

3. Alianzas comerciales y comercio electrónico más seguros.

4. Mayor confianza en el cliente.

5. Auditorías de seguridad más precisas y confiables.

6. Menor responsabilidad civil.

CAPÍTULO 2

ANÁLISIS DEL RIESGO DE SEGURIDAD

2.1 Definiciones

Ya que no existe una seguridad total y las medidas de seguridad no pueden asegurar al 100% la protección en contra de las vulnerabilidades, es imprescindible realizar periódicamente en una organización, un análisis del riesgo para identificar las consecuencias probables o los riesgos asociados con las vulnerabilidades, y así, lograr un manejo del riesgo tras la implementación y el mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable.

El proceso de análisis del riesgo le da al manejo del riesgo la información necesaria para hacer juicios sobre la seguridad de la información de cierta organización. Este procedimiento identifica los controles de seguridad existentes, calcula vulnerabilidades y evalúa el efecto de las amenazas en cada área vulnerable, en la mayoría de los casos, el análisis del riesgo intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos.

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

1. Activo: es todo aquello con valor para una organización y que necesita protección - datos, infraestructura, hardware, software, personal y su experiencia, información, servicios.

2. Riesgo: posibilidad de sufrir algún daño o pérdida.

3. Aceptación del riesgo: decisión para aceptar un riesgo.

4. Análisis de riesgo: uso sistemático de información disponible para identificar las fuentes y para estimar qué tan seguido determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias. Uso sistemático de la información para describir y/o calcular el riesgo (Tabla 2.1). Evaluación de amenazas y vulnerabilidades de la información y su impacto (ver tabla 2.2) en el procesamiento de la información así como su frecuencia de ocurrencia (ver tabla 2.3).

Cálculo del riesgo (probabilidad x daño)	Clasificación
0	Ninguna
1-3	Baja
4-7	Media
8-14	Alta
15-19	Crítica
20-30	Extrema

Tabla 2.1. Un ejemplo de la escala del riesgo

Daño del acontecimiento	Grado del daño	Clasificación
Insignificante	Sin impacto	0
Menor	No se requiere un esfuerzo extra para reparar	1
Significante	Daño tangible, esfuerzo extra requerido para reparar	2
Dañino	Gasto significante requerido de recursos Daño a la reputación y a la confianza	3
Serio	Pérdida de la conexión Compromiso de grandes cantidades de datos o servicios	4
Grave	Apagado permanente Compromiso total	5

Tabla 2.2. Un ejemplo del impacto del acontecimiento

Acontecimiento	Frecuencia	Clasificación
Insignificante	Sin probabilidad de que ocurra	0
Muy bajo	2-3 veces cada 5 años	1
Bajo	< = una vez por año	2
Medio	< = una vez cada 6 meses	3
Alto	< = una vez por mes	4
Muy alto	> = una vez por mes	5
Extremo	> = una vez por día	6

Tabla 2.3. Un ejemplo de la frecuencia de ocurrencia de un acontecimiento

Es importante mencionar que los dueños de la información son quienes la jerarquizan, establecen un valor a cada activo e identifican lo que le costaría a la organización en caso de existir pérdidas de información, por lo que una organización puede basarse en la experiencia o en métodos estadísticos para crear tablas como los ejemplos anteriores.

5. Manejo del riesgo: proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar sistemas de información por un costo aceptable.

6. Evaluación del riesgo: comparación de los resultados de un análisis del riesgo con criterios estándares del riesgo u otros criterios de decisión.

7. Impacto: pérdidas como resultado de la actividad de una amenaza, las pérdidas son normalmente expresadas en una o más áreas de impacto - destrucción, denegación de servicio, revelación o modificación.

8. Pérdida esperada: el impacto anticipado y negativo a los activos debido a una manifestación de la amenaza.

9. Vulnerabilidad: una condición de debilidad.

10. Amenaza: una acción potencial[7] con la posibilidad de causar daño.

11. Riesgo residual: el nivel de riesgo que permanece tras considerar todas las medidas necesarias, los niveles de vulnerabilidad y las amenazas relacionadas. Éste debe aceptarse tal como es o reducirse a un punto donde pueda ser aceptado

12. Control: son los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización. Un mismo control puede ser implementado para una o varias políticas de seguridad, lo cual indica que la relación forzosamente no es uno a uno.

[7] Que puede suceder o existir, pero no existe aún.

Un **análisis del riesgo de seguridad** es un procedimiento para estimar el riesgo de los activos de cómputo y su pérdida debido a la manifestación de las amenazas. El procedimiento primero determina el nivel de vulnerabilidad del activo tras identificar y evaluar el efecto de los controles implantados en el lugar. Un nivel de vulnerabilidad del activo para cierta amenaza se determina con controles que se encuentran en el lugar en el momento en el que se realiza el análisis del riesgo. A continuación, información detallada acerca del activo se utiliza para determinar el significado de las vulnerabilidades sobre dicho activo, esto incluye cómo es o será utilizado, los niveles de sensibilidad de los datos (véase la tabla 2.4), misión crítica, interconectividad, etc. Finalmente el impacto negativo al activo se estima tras examinar varias combinaciones de amenazas y áreas de vulnerabilidad.

Nivel	Clasificación
0	No clasificado
1	Información delicada no clasificada
2	Confidencial
3	Secreta
4	Secreta con una categoría
5	Ultrasecreta sin categorías o secreta con dos o más categorías
6	Ultrasecreta con una categoría
7	Ultrasecreta con dos o más categorías

Tabla 2.4. Un ejemplo del nivel de sensibilidad de los datos

Un análisis del riesgo de seguridad define el ambiente actual y realiza acciones correctivas recomendadas si el riesgo residual no es aceptable, es una parte vital de cualquier programa de manejo del riesgo y la seguridad. El proceso de análisis del riesgo debe realizarse con suficiente regularidad para asegurar que cada aproximación del manejo del riesgo de la organización sea una respuesta real a los riesgos actuales que se encuentran asociados con la información de sus activos. El manejo del riesgo debe decidir si acepta el riesgo residual o implementa las acciones recomendadas.

Las relaciones entre los elementos de un análisis del riesgo se muestran en la figura 2.1.

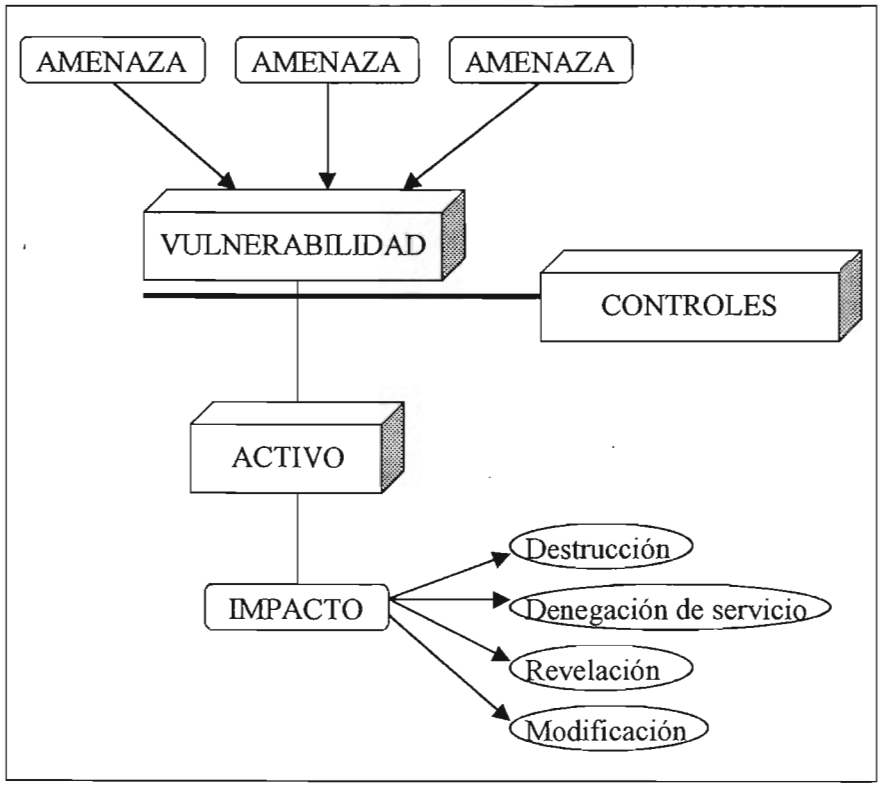

Figura 2.1. Relaciones entre los elementos de un análisis del riesgo

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

a) Identificar, evaluar y manejar los riesgos de seguridad.

b) Estimar la exposición de un recurso a una amenaza determinada.

c) Determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.

d) Tomar mejores decisiones en seguridad de la información.

e) Enfocar recursos y esfuerzos en la protección de los activos.

2.2 Tipos

La seguridad en cualquier sistema debe guardar una proporción con respecto a sus riesgos. Sin embargo, el proceso para determinar qué controles de seguridad son apropiados y rentables, es a menudo una cuestión compleja y a veces subjetiva. Una de las principales funciones del análisis del riesgo de seguridad es poner este proceso sobre una base más objetiva.

Existen dos tipos esenciales del análisis del riesgo:

1. **Análisis cuantitativo del riesgo:** todos los activos, sus recursos y los controles se identifican, y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema de tal forma que se identifiquen las áreas que son sensibles.

   Posteriormente, el análisis cuantitativo del riesgo hace uso del término Expectativa de Pérdida Anual (ALE) o Costo Anual Estimado (EAC), el cual se calcula para un cierto acontecimiento simplemente multiplicando la frecuencia de la ocurrencia de la amenaza por el valor del activo o clasificación del daño. Para esto, es necesario recolectar con detalle estimaciones exactas utilizando técnicas matemáticas y estadísticas.

   De esta forma se puede decidir si los controles existentes son adecuados o si se requiere la implementación de otros – esto se observa cuando el producto obtenido tras multiplicar el valor del activo por la frecuencia de la ocurrencia de la amenaza en un periodo de tiempo determinado por la duración del control, es menor que el costo de dicho control.

   Es teóricamente posible situar acontecimientos en el orden del riesgo ALE y posteriormente tomar las decisiones más convenientes. Los problemas con este tipo de análisis del riesgo se asocian generalmente a la falta de fiabilidad[8] y a la inexactitud de los datos, debido a que es difícil lograr una figura representativa de la pérdida o daño que se tiene como resultado de las brechas de

[8] Probabilidad del buen funcionamiento de una cosa.

seguridad. La probabilidad raramente es exacta y en algunos casos es capaz de promover la satisfacción personal. Además, los controles a menudo abordan acontecimientos potenciales que se correlacionan con frecuencia.

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

Ambos tipos del análisis del riesgo hacen uso de los siguientes elementos interrelacionados:

a) **Amenazas:** una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad. Es todo aquello que intenta o pretende destruir. Las amenazas están siempre presentes en cada sistema.
Las amenazas provienen de diversas fuentes, entre ellas se pueden mencionar las siguientes:

   i) **De humanos**: la amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad (cuando un empleado es despedido). Ejemplo de una amenaza por ignorancia: se da cuando acaban de contratar a una persona en una organización y su nuevo trabajo consiste en dar mantenimiento a la base de datos de los clientes de la empresa, la persona podría llegar a borrar todos los registros de la base de datos (sin querer) debido a que no lo capacitaron o desconoce (ignora) el proceso para dar mantenimiento a la base de datos.

   ii) **Errores de Hardware:** se da la amenaza por fallas físicas que presente cualquier elemento de los dispositivos que conforman a la computadora. Los problemas más identificados para que el suministro de energía falle (hay que recordar que si no fluye corriente a través de los elementos de los dispositivos de la

computadora, ésta no funciona) son el bajo voltaje, ruido electromagnético, distorsión, alto voltaje, variación de frecuencia, etc. Ejemplo: Un bajo voltaje que reciba la fuente de alimentación de la computadora, al momento de estar respaldando información, seguramente se apagaría la computadora perdiendo de esa manera la información que se estaba respaldando.

iii) **Errores de la Red:** se presenta una amenaza cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación, es decir, que un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red. Otro factor es la desconexión del canal. Por ejemplo: cuando uno o varios usuarios están conectados a la red, si el canal se llega a desconectar por cualquier razón (corte del cable), el sistema operativo debe inmediatamente dar de baja del sistema a los usuarios o almacenar los datos, en un archivo, de los usuarios desconectados; de tal manera que se obligue nuevamente a que se firmen en la red para obtener otra vez el control.

iv) **Problemas de tipo lógico:** la amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad, se implementa mal, es decir, no cumplió con las especificaciones del diseño. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita enviar y recibir información, ésta podría consistir en enviar contraseñas y recibir el mensaje de contraseña válida; dándole al intruso elementos para un posible ataque. El paso de parámetros en una función, que se utilice para la verificación de contraseñas de los usuarios, representa una amenaza cuando se intenta tener registros apuntando a localidades que contienen los parámetros, es más seguro pasar los parámetros directamente en registros. Ejemplo: en la mayoría de los sistemas, los usuarios no pueden determinar si el hardware o el software con que funcionan son los que se supone que deben ser. Esto facilita al intruso para que pueda reemplazar un programa sin conocimiento del usuario y éste pueda inadvertidamente teclear su contraseña en un programa de entrada falso.

v) **Desastres:** las amenazas de este tipo surgen de las fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir amenazas directas, pues repercute indiscutiblemente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etc. Ejemplo: En organizaciones donde cuentan con un centro de cómputo, es muy importante mantener toda el área donde está localizada el equipo (computadoras, servidores, mainframes, etc.) a la temperatura que los fabricantes de los equipos especificaron para el buen desempeño de los mismos.

b) **Vulnerabilidades:** una vulnerabilidad es una debilidad que puede ser explotada para violar la seguridad. Las vulnerabilidades son también extremadamente variadas. Una administración pobre es un problema común que llega a ser grave cuando se acopla con una vulnerabilidad. Por ejemplo, los productos que son liberados con configuraciones inseguras. Un sistema operativo puede tener una arquitectura o un diseño defectuoso; muchos sistemas están expuestos a "agujeros" de seguridad que son explotados por los perpetradores[9] para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de comunicación, navegadores de Internet, correo electrónico y toda clase de servicios en LAN's o WAN's. En lo que respecta al hardware, también puede tener defectos que puedan ser explotados para violar la seguridad. Las vulnerabilidades permiten que un sistema sea más propenso a ser atacado por una amenaza o que un ataque tenga mayor probabilidad de tener cierto éxito o impacto.

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

i) Los controles disuasivos reducen la probabilidad de un ataque deliberado.

ii) Los controles preventivos protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.

[9] Un perpetrador es aquel individuo que se basa en cualquier medio para ejecutar o consumar un delito o culpa grave.

iii) Los controles correctivos reducen el efecto de un ataque.

iv) Los controles detectores descubren ataques y disparan controles preventivos o correctivos.

Estos tres elementos pueden ilustrarse mediante un modelo relacional simple que se aprecia en la figura 2.2.

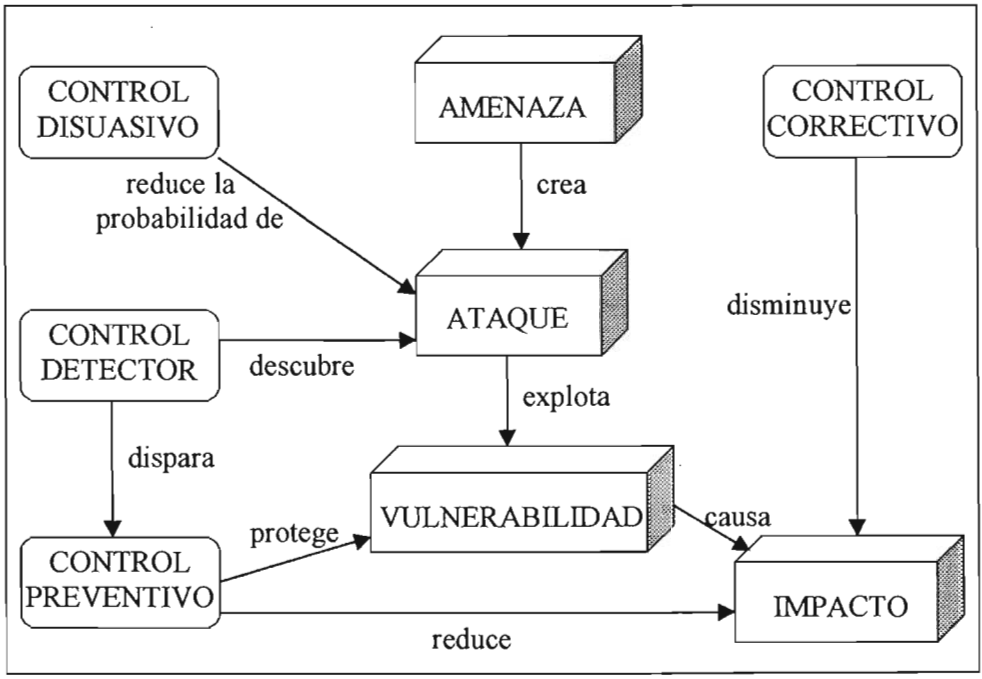

Figura 2.2. Modelo relacional simple

En ocasiones el costo de algunos controles resulta ser mayor que el activo que se desea proteger o la pérdida es mínima si no se cuenta con el control, en estos casos lo más conveniente es adquirir un seguro que cubra el valor del daño cuando éste se presente.

Algunas herramientas que permiten realizar el análisis de riesgo son:

- COBRA
  http://www.security-risk-analysis.com/

- CRAMM
  http://www.insight.co.uk/cramm/

- CORA
  http://www.ist-usa.com/

- The Buddy System
  http://www.buddysystem.net/

- RiscPAC
  http://www.csciweb.com/

2.3 Cómo establecer los requerimientos de seguridad

Existen tres fuentes principales que deben considerarse para que una organización identifique sus requerimientos de seguridad:

a) La primera fuente se deriva de la determinación de los riesgos de la organización. A través de la evaluación del riesgo se identifican las amenazas a los activos y la vulnerabilidad de éstos, también se evalúa la probabilidad de ocurrencia y se estima el potencial de impacto.

b) La segunda fuente se refiere a los requerimientos legales, regulatorios, contractuales y establecidos que una organización, sus socios comerciales, contratistas y proveedores de servicio tienen que satisfacer.

c) La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para el procesamiento de la información que una organización ha desarrollado para mantener sus operaciones.

2.4 Determinar los riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de riesgos de seguridad. El gasto en los controles necesita balancearse en comparación con el daño al negocio como resultado de las fallas de seguridad. Las técnicas de evaluación de riesgo pueden aplicarse a toda la organización, o sólo en algunas partes, como en los sistemas

individuales de información, componentes específicos del sistema o servicios donde esto es factible, realista y útil.

La evaluación del riesgo es una consideración sistemática de:

a) El daño al negocio, ya que es probablemente debido a una falla de seguridad, tomando en cuenta las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos.

b) La probabilidad real de la ocurrencia de una falla ante amenazas y vulnerabilidades comunes y de controles recientemente implementados.

Los resultados de esta evaluación ayudan a guiar y determinar la acción apropiada de administración y las prioridades para manejar los riesgos de seguridad de la información, también permitirán implementar los controles seleccionados para proteger contra esos riesgos. El proceso de determinación de riesgos y selección de controles necesita ejecutarse varias veces para cubrir diferentes partes de la organización o sistemas individuales de información.

Es importante realizar revisiones periódicas de riesgos de seguridad y controles implementados para:

a) Tomar en cuenta los cambios de requerimientos del negocio y las prioridades.

b) Considerar nuevas amenazas y vulnerabilidades.

c) Confirmar que los controles son efectivos y apropiados.

Las revisiones deben ejecutarse en diferentes niveles de profundidad dependiendo de los resultados de evaluaciones previas y de los niveles cambiantes de riesgo que la administración está preparada para aceptar. Las evaluaciones de riesgo son generalmente verificadas primero en un nivel alto, como un medio para establecer la prioridad de los recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado para analizar los riesgos específicos.

2.5 Pasos del análisis del riesgo

Cualquier análisis del riesgo de seguridad debe indicar:

1. El nivel actual de riesgo.

2. Las consecuencias probables.

3. Qué hacer con el riesgo residual si es muy alto.

Para ser útil, una metodología de análisis del riesgo debe producir una sentencia cuantitativa del impacto de un riesgo o del efecto de los problemas específicos de seguridad. Los tres elementos principales en un análisis de riesgo son:

1. Un balance del impacto o del costo de alguna dificultad específica si ésta sucede.

2. Una medida de la efectividad de los controles que se encuentran en el lugar.

3. Una serie de recomendaciones para corregir o minimizar los problemas identificados.

La planeación para la seguridad de la información y del manejo del riesgo empieza con la identificación de los activos de seguridad, la sensibilidad de los datos, los valores, los controles dentro del lugar, la configuración del sistema o proyecto, amenazas probables y su frecuencia de ocurrencia. Esta información se utiliza posteriormente para calcular las vulnerabilidades y los riesgos. El proceso de análisis del riesgo consta de ocho pasos interrelacionados:

1. **Identificar y evaluar los activos:** el primer paso para todas las evaluaciones del riesgo es identificar y asignar un valor a los activos que necesitan protección. El valor de los activos es un factor significante en la decisión para realizar cambios operacionales o para incrementar la protección de los activos. El valor del activo se basa en su costo, sensibilidad, misión crítica, o la combinación de estas propiedades. Cuando el valor se basa en algo más que el costo, generalmente se utiliza una tabla estándar de equivalencia para obtener su valor monetario correspondiente. El valor del activo será

utilizado más tarde para determinar la magnitud de pérdida cuando la amenaza ocurra.

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

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

4. **Determinar el impacto de la ocurrencia de una amenaza:** cuando la explotación de una amenaza ocurre, los activos sufren cierto impacto. Las pérdidas son catalogadas en áreas de impacto llamadas:

   a) Revelación: cuando la información es procesada y se pierde la confidencialidad.

   b) Modificación: el efecto de la manifestación de una amenaza cambia el estado original del activo.

   c) Destrucción: se logra la pérdida completa del activo.

   d) Denegación de servicio: pérdida temporal de los servicios.

5. **Controles en el lugar:** el crédito debe darse a los controles en el lugar. La identificación de los controles es parte del proceso de recolección de datos en cualquier proceso de análisis del riesgo. Existen dos tipos principales:

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

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

6. **Determinar los riesgos residuales (conclusiones):** siempre existirá un riesgo residual, por lo tanto, debe determinarse cuándo el riesgo residual es aceptable o no. El riesgo residual toma la forma de las conclusiones alcanzadas en el proceso de evaluación. Las conclusiones deben identificar:

   a) Las áreas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de la amenaza.

   b) Todos los controles que no están dentro del lugar.

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

7. **Identificar los controles adicionales (recomendaciones):** una vez que el riesgo residual se haya determinado, el siguiente paso es identificar la forma más efectiva y menos costosa para reducir el riesgo a un nivel aceptable. Un intercambio operacional – el cual puede tomar la forma de costo, conveniencia, tiempo, o una mezcla de los anteriores – debe realizarse al mismo tiempo que los controles adicionales son implementados. Las recomendaciones son:

   a) Recomendación de controles requeridos: controles requeridos u obligatorios que no se encuentran en el lugar son la primera recomendación.

   b) Recomendación de controles discrecionales: la segunda recomendación generalmente identifica los controles discrecionales necesarios para reducir el nivel de riesgo.

8. **Preparar un informe del análisis del riesgo:** el proceso de análisis del riesgo ayuda a identificar los activos de información en riesgo y añade un valor a los riesgos, adicionalmente identifica medidas protectoras y minimiza los efectos del riesgo y asigna un costo a cada control. El proceso de análisis del riesgo también determina si los controles son efectivos. Cuando el análisis está completo, debe prepararse un informe de la evaluación del riesgo. Los detalles técnicos del reporte deben incluir como mínimo:

   a) Niveles de vulnerabilidad.

   b) Amenazas correspondientes y su frecuencia.

   c) El ambiente usado.
   d) Conexión del sistema.

   e) Nivel o niveles de sensibilidad de los datos

   f) Riesgo residual, expresado en una base individual de vulnerabilidad.

   g) Cálculos detallados de la Expectativa de Pérdida Anual.

El análisis del riesgo de seguridad es fundamental en la seguridad de cualquier organización. Es esencial asegurarse que los controles y el gasto que implican sean completamente proporcionales a los riesgos a los cuales se expone la organización.

CAPÍTULO 3

SECCIONES DEL ESTÁNDAR ISO 17799

El estándar ISO 17799 sugiere que los requerimientos de seguridad se identifiquen mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debe balancearse con el daño que presente el negocio como consecuencia de las fallas de seguridad. El proceso para determinar los riesgos y seleccionar los controles, en ciertas ocasiones, debe realizarse varias veces para cubrir diversas áreas de la organización o sistemas de información individuales y es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados.

3.1 Selección de controles

Una vez que se hayan identificado los requerimientos de seguridad, los controles del estándar ISO 17799 deben seleccionarse e implementarse para asegurar que los riesgos se reducen a un nivel aceptable. Los controles se escogen con base en el costo de implementación en relación con los riesgos que se reducen y a las pérdidas potenciales si ocurre una brecha en la seguridad. Los factores no monetarios, tales como pérdida de reputación, también se deben considerar. Los controles pueden servir como una guía de principios que proveen un buen punto de partida para implementar la seguridad de la información ya que se basan en requerimientos legislativos esenciales o son considerados como la mejor práctica para la seguridad de la información.

Los controles esenciales para una organización desde un punto de vista legislativo incluyen:

a) Protección de datos y confidencialidad de la información personal.

b) Resguardo de los registros de la organización.

c) Derechos de propiedad intelectual.

Los controles considerados como la mejor práctica para la seguridad de la información incluyen:

a) Documento de la política de seguridad de la información.

b) Asignación de las responsabilidades de la seguridad de la información.

c) Capacitación y educación en seguridad de la información.

d) Reporte de los incidentes de seguridad.

e) Manejo de la continuidad del negocio.

Estos controles aplican en la mayoría de las organizaciones, la relevancia de cualquier control debe determinarse dependiendo de los riesgos específicos que la organización enfrente.

Los siguientes factores son críticos para una aplicación exitosa de la seguridad de la información dentro de una organización:

a) Política de seguridad, objetivos y actividades que reflejan los objetivos del negocio.

b) Una aproximación para implementar la seguridad que es consistente con la cultura de la organización.

c) Apoyo visible y compromiso de la administración.

d) Un buen entendimiento de los requerimientos de seguridad, evaluación del riesgo y manejo del riesgo.

e) Mercado efectivo de seguridad para todos los administradores y empleados.

f) Distribución de guías sobre política de seguridad de la información y estándares a todos los empleados y contratistas.

g) Abastecimiento apropiado de capacitación y educación.

h) Un sistema de medición balanceado, el cual es utilizado para evaluar el desempeño en el manejo de la seguridad de la información y retroalimentar sugerencias para su mejoramiento.

3.2 Secciones de seguridad

Las organizaciones diariamente enfrentan amenazas a sus activos de información, al mismo tiempo, ellas llegan a ser dependientes de esos

recursos. Muchos sistemas de información no son seguros y las soluciones técnicas son sólo una aproximación a la seguridad de la información.

Establecer los requerimientos de seguridad de la información es esencial, pero para hacer eso, las organizaciones deben entender su único y propio ambiente de amenazas. Los ambientes de amenazas se determinan mediante la ejecución de una evaluación sistemática de riesgos de seguridad. Una vez que las áreas de riesgo se identifican, los controles apropiados se seleccionan para mitigar esos factores de riesgo.

El estándar ISO 17799 contiene diez secciones de seguridad – cada una cubre un diverso asunto o área -, las cuales son utilizadas como base para la determinación de los riesgos de seguridad y la aplicación de controles de seguridad para el manejo de la seguridad de la información. Estas secciones son:

1. Política de seguridad.
2. Seguridad de la organización.
3. Clasificación y control de activos.
4. Seguridad del personal.
5. Seguridad física y ambiental.
6. Gestión de comunicaciones y operaciones.
7. Control de acceso.
8. Desarrollo y mantenimiento de sistemas.
9. Plan de continuidad del negocio.
10. Cumplimiento.

3.2.1 Política de seguridad

El objetivo de esta sección es:

- Proporcionar a la dirección o administración ayuda para la seguridad de la información.

La **política de seguridad**, en el mundo real, es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política especifica qué propiedades de seguridad el sistema debe proveer. De manera similar, la política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

Una **política de seguridad informática** debe fielmente representar una política del mundo real y además debe interactuar con la política de recursos, por ejemplo, políticas en el manejo de bases de datos o de transacciones. En ella, se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas. Así mismo debe ser expresada en un lenguaje en el que todas las personas involucradas (quienes crean la política, quienes la van a aplicar y quienes la van a cumplir) puedan entender.

Esta primera sección trata la administración, el compromiso y la dirección para lograr las metas de seguridad de la información, e incluye[10]:

a) **Documento de la política de seguridad de la información:** una política de seguridad debe estar especificada en un documento especial para tal propósito, redactada en un lenguaje natural, claramente y sin ambigüedades posibles. El documento deberá especificar cuáles son las metas de seguridad de la organización, qué propiedades de seguridad se pretenden cubrir con la aplicación

[10] Para información más detallada véase cada inciso en el Apéndice A.

de las políticas y la manera de usarlas. Este documento, junto con una jerarquía de estándares, principios y procedimientos, ayuda a implementar y reforzar los enunciados de la política, además debe aprobarse por la administración, publicarse y comunicarse, de manera apropiada a todos los empleados, también debe expresar el compromiso y la aproximación de la organización para manejar la seguridad de la información.

b) **Propiedad y análisis:** el compromiso de administración de seguridad de la información se establece al asignar planes de propiedad y análisis del documento de la política de seguridad de la información. La política debe tener un propietario, éste es el responsable de su mantenimiento y revisión de acuerdo a un proceso definido, dicho proceso debe asegurar una revisión periódica debido a los cambios que afectan la evaluación original del riesgo, por ejemplo, incidentes significativos de seguridad, nuevas vulnerabilidades o cambios a la infraestructura técnica o de la organización.

La importancia de esta primera sección ha llevado a que algunas organizaciones internacionales se dediquen ha desarrollar documentos que contienen un amplio conjunto de políticas de seguridad, su objetivo principal es agrupar la mayor cantidad de políticas utilizadas en un cierto ámbito y que cumplan con estándares internacionales.

Una manera inicial de ocuparse de las políticas de seguridad es utilizar algunas políticas preescritas como base, sin embargo, es de suma importancia considerar que aquéllas que se hayan elegido deben cumplir con la misión de la organización, sus objetivos, el ámbito de la misma – educativo, gubernamental, industrial, comercial... – y el estándar al que desea apegarse, por lo que las políticas deben modificarse – de ser necesario – para adaptarse a la organización.

También debe tomarse en cuenta que 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 a las organizaciones modernas.

Algunos acervos de políticas de seguridad preescritas se listan a continuación:

1. Proyecto de política de seguridad del Instituto SANS
   http://www.sans.org/resources/policies/

2. Centro de recursos de seguridad en cómputo del Instituto NIST
   http://csrc.nist.gov/policies/

3. Wood, Charles Cresson. Information Security Policies Made Easy Version 4.
   http://www.cse-cst.gc.ca/en/documents/publications/gov_pubs/itspsr/cipr10.pdf

4. Políticas de seguridad para personal de empresas proveedoras
   https://www.ejie.es/proveedores/datos/polit_prov.pdf

5. Políticas para la universidad
   http://security.arizona.edu/policies-guidelines.html#policies

6. Política de seguridad en Internet
   http://secinf.net/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Sample_Policy_Areas.html

7. Política de seguridad de Tecnología de la Información
   http://www.ruskwig.com/docs/security.doc

8. Política de seguridad del usuario
   http://www.ruskwig.com/docs/user.doc

9. Wood, Charles Cresson. *Information Security Policies Made Easy Version 9*, PentaSafe Security Technologies, 2002

10. The RUSecure™ Information Security Policies
    http://www.information-security-policies.com/download.htm

Es necesario mencionar, que en las secciones siguientes las políticas de seguridad que aparecen, fueron tomadas del documento citado como última fuente, ya que éstas cumplen con el estándar ISO 17799.

3.2.2 Seguridad de la organización

Los objetivos de esta sección son:

- Manejar la seguridad de la información dentro de la compañía.
- Mantener la seguridad de los recursos de la organización, del tratamiento de la información y de los activos de información a los que terceras entidades tienen acceso.
- Mantener la seguridad de la información cuando el procesamiento de la información ha sido responsabilidad de un outsourcing (organización externa).

Esta segunda sección trata la necesidad de mantener un marco que cree, sostenga y maneje la infraestructura de la seguridad, e incluye[11]:

a) **Foro para el manejo de la seguridad de la información:** provee un comité multidisciplinario encargado de discutir y diseminar problemas de seguridad de la información en toda la organización. La seguridad de la información es una responsabilidad del negocio que comparten todos los miembros del grupo administrativo. Un foro asegura la existencia de una dirección clara y un soporte visible para manejar las iniciativas de seguridad que deben considerarse, este foro debe promover la seguridad en la organización a través de un compromiso apropiado y un recurso adecuado.

b) **Coordinación del sistema de seguridad de la información:** actúa como un punto central de contacto para los problemas de seguridad, tratamiento y decisiones. En una organización, es necesaria la formación de un grupo de representantes administrativos de partes relevantes de la organización para coordinar la implementación de los controles de seguridad de la información.

c) **Responsabilidades de la seguridad de la información:** las responsabilidades individuales de la seguridad de la información se localizan y detallan de manera no ambigua en las actividades de trabajo. Deben definirse claramente responsabilidades para la

[11] Para información más detallada de algunos incisos, véase el Apéndice B.

protección de los activos individuales y para llevar a cabo procesos específicos de seguridad. La política de seguridad de la información provee una guía general sobre la asignación de los roles de seguridad y las responsabilidades de la organización, ésta debe complementarse cuando sea necesario y detallarse para sitios, sistemas o servicios específicos. Es obligatorio definir claramente responsabilidades locales para objetos físicos individuales, activos de información y procesos de seguridad, como el plan de continuidad del negocio.

d) **Procesos de autorización:** aseguran que se evalúan las consideraciones de seguridad y se obtienen las aprobaciones para los sistemas de procesamiento de información que son nuevos y/o modificados.

e) **Especialista en seguridad de la información:** mantiene relaciones con especialistas independientes para permitir el acceso a la experiencia práctica que no se encuentra disponible dentro de la organización. Los especialistas proveen consejos en todos los aspectos de seguridad de la información usando su propia experiencia o la externa. La calidad de su evaluación de amenazas de seguridad y su asesoramiento en los controles determinarán la efectividad de la seguridad de la información de la empresa, para una mayor efectividad e impacto, se le debe permitir el acceso a la administración de toda la empresa. Debe consultarse a un especialista de manera oportuna después de la ocurrencia de un incidente de seguridad o al identificar una brecha en la seguridad, ya que provee una guía experta o recursos para la investigación, dicho especialista puede conducir o aconsejar la investigación.

f) **Cooperación administrativa:** mantiene relaciones con los socios que comparten información y las autoridades locales que aplican las leyes. Deben mantenerse contactos apropiados con autoridades que aplican la ley, cuerpos reguladores, proveedores del servicio de información y operadores de telecomunicaciones para asegurar que se toma una acción apropiada y se obtiene rápidamente un consejo cuando ocurre un incidente de seguridad. Se aconseja considerar una membresía en grupos de seguridad y en foros de la industria. Los intercambios de información deben restringirse para evitar que la

información confidencial de la organización se otorgue a personas sin autorización.

g) **Análisis independiente:** mecanismos que permiten el análisis local de la efectividad de la seguridad. El documento de la política de la seguridad de la información precisa la política y las responsabilidades de seguridad de la información, su puesta en práctica se debe revisar de manera independiente para asegurar que las prácticas de la organización reflejan correctamente la política, y que ésta es factible y eficaz. Tal revisión se puede realizar mediante un área interna, un administrador independiente o una tercera organización especialista en tales revisiones, donde éstos cuentan con las habilidades y la experiencia apropiadas.

h) **Acceso de la tercera entidad:** mecanismos para gobernar la interacción de la tercera entidad dentro de la organización basada en los requerimientos del negocio. Se busca mantener la seguridad de los medios de procesamiento de información de la organización y de los activos de la información a los que tienen acceso las terceras entidades. Debe controlarse el acceso de terceros a los medios de procesamiento de información de la organización si se presenta la necesidad de que exista tal acceso, es necesario realizar una evaluación del riesgo para determinar implicaciones de la seguridad y requerimientos de control. Los controles se deben convenir y definir en un contrato con los terceros. El acceso de los terceros puede también implicar a otros participantes, por esto, en los contratos que confieren a terceras entidades se incluye el permiso para la designación de otros participantes y las condiciones para su acceso.

i) **Outsourcing (organización externa):** las medidas administrativas del outsourcing deben tener requerimientos de seguridad claros y estipulados por contrato. Busca mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información la maneja otra organización. Las acciones del outsourcing en el contrato entre las entidades deben tratar los riesgos, los controles de seguridad y los procedimientos para los sistemas de información, las redes y/o los ambientes de escritorio.

Las siguientes políticas[12] son algunos ejemplos que sirven para esta segunda sección, cabe aclarar que no son las únicas que existen:

- N° 030202 Administración de sistemas: "Los administradores del sistema deben estar capacitados y contar con experiencia en los sistemas y plataformas que utiliza la organización. Además, deben informarse y familiarizarse con el alcance que tienen los riesgos de seguridad de la información y cómo deben manejarse."

- N° 010103 Colocación del nuevo hardware: "Todas las nuevas colocaciones de hardware deben planearse formalmente y se les debe notificar las fechas de colocación a todas las entidades involucradas y encargadas para ello. Los requerimientos de seguridad de la información de las nuevas colocaciones deben entregarse a todas las entidades involucradas para que éstas las conozcan y se logre una colocación adecuada."

3.2.3 Clasificación y control de activos

El objetivo de esta sección es:

- Mantener la protección apropiada de activos corporativos y asegurarse de que los activos de la información reciben un nivel apropiado de protección.

Se consideran todos los activos importantes de la información y se les nombra un dueño. La responsabilidad sobre los activos asegura una protección apropiada, para esto, se identifican los dueños de todos los activos importantes y se les asigna la responsabilidad del mantenimiento de controles adecuados, sin embargo, la responsabilidad de implementar controles puede delegarse, aunque ésta siempre debe permanecer con el dueño del activo que se haya nombrado.

Esta tercera sección trata la capacidad de la infraestructura de la seguridad para proteger los activos de la administración, e incluye[13]:

[12] Extraídas del documento The RUSecure™ Information Security Policies.
[13] Para información más detallada véase cada inciso en el Apéndice C.

a) **Responsabilidad e inventario:** mecanismos para mantener un inventario preciso de los recursos y establecer su pertenencia y responsabilidad. Los inventarios de activos ayudan a asegurar la protección eficaz del activo, y se pueden requerir para otros propósitos del negocio, tales como salud y seguridad, seguro o razones financieras - administración del activo. El proceso para compilar un inventario de activos es un aspecto importante de la administración del riesgo, una organización debe ser capaz de identificar sus activos, el valor y la importancia relativos a éstos. De acuerdo con esta información, una organización puede entonces proporcionar los niveles de protección conmensurados con el valor y la importancia de los activos, un inventario debe elaborar y mantener los activos importantes asociados a cada sistema de información, cada activo debe identificarse y su propiedad y clasificación de seguridad convenida se tiene que documentar claramente, junto con su localización actual - esto es importante cuando se trata de recuperar debido a una pérdida o daño.

b) **Clasificación:** mecanismos para clasificar los recursos con base en el impacto del negocio. Las clasificaciones y los controles asociados a la información deben tomar en cuenta las necesidades del negocio para compartir o restringir la información y los impactos asociados a tales necesidades, por ejemplo, el acceso no autorizado o daños a la información. En general, la clasificación que se le da a la información es una manera de determinar cómo se dirige y protege.

c) **Etiquetado y manejo:** el manejo de estándares, incluyendo introducción, transferencia, eliminación y disposición de los activos, se basa en la clasificación de recursos, es importante definir un conjunto apropiado de procedimientos para etiquetar y manejar la información de acuerdo con el esquema de clasificación adoptado por la organización; estos procedimientos necesitan cubrir activos de información en formatos físicos y electrónicos.

Las siguientes políticas[14] son algunos ejemplos que sirven para esta tercera sección, cabe aclarar que no son las únicas que existen:

[14] Extraídas del documento The RUSecure™ Information Security Policies.

- N° 010602 Mantenimiento de un inventario o registro de hardware: "Debe mantenerse un inventario formal de hardware de todo el equipo y es necesario actualizarlo todo el tiempo."

- N° 030518 Uso de nombres significativos para los archivos: "El nombre de los archivos de datos de la organización debe ser significativo y los usuarios deben ser capaces de reconocerlo."

3.2.4 Seguridad del personal

Los objetivos de esta sección son:

- Reducir riesgos de error, hurto, fraude o el mal uso por parte del recurso humano.

- Asegurarse de que los operadores estén enterados de las amenazas, se preocupen por la seguridad de la información, y que estén equipados para utilizar la política corporativa de seguridad en el transcurso de su trabajo normal.

- Reducir al mínimo el daño de incidentes, el mal funcionamiento de la seguridad y aprender de tales incidentes.

Las responsabilidades de seguridad se deben tratar en la etapa de reclutamiento de personal, incluirse en los contratos, y supervisarse durante la colocación del individuo. Los reclutas potenciales deben seleccionarse de manera adecuada, especialmente para los trabajos sensibles. Todos los empleados y terceras entidades que hacen uso de los medios para el procesamiento de la información deben firmar un acuerdo de confidencialidad (no divulgación).

Esta cuarta sección trata la capacidad de la organización para mitigar el riesgo inherente en las interacciones humanas, e incluye[15]:

a) **Proyección personal:** políticas entre marcos legales y culturales que determinan la adaptabilidad y capacidad de todo el personal con acceso a los recursos de la organización. Este marco debe estar basado en descripciones del trabajo y/o clasificación de recursos.

[15] Para información más detallada véase cada inciso en el Apéndice D.

Los papeles y las responsabilidades de seguridad, según lo establecido en la política de seguridad de la información de la organización, deben documentarse de manera apropiada e incluir cualquier responsabilidad general para implementar o mantener la política de seguridad vigente, así como cualquier responsabilidad específica para proteger activos en particular, o para implementar actividades o procesos específicos de seguridad.

b) **Responsabilidades de seguridad:** al personal se le debe informar cuáles son sus responsabilidades de seguridad, incluyendo códigos de conducta y acuerdos de no divulgación, para indicar que la información es confidencial o secreta, se utilizan acuerdos de confidencialidad o de no divulgación. Es importante que los empleados firmen tales acuerdos como parte de los términos y condiciones iniciales de empleo, los usuarios externos o el personal ocasional que no están cubiertos por un contrato existente (que contiene el acuerdo de confidencialidad) deben firmar un acuerdo de confidencialidad antes de que se les dé el acceso a los medios de procesamiento de la información. Los acuerdos de confidencialidad necesitan revisarse cuando hay cambios en los términos del empleo o del contrato, particularmente cuando los empleados se van de la organización o los contratos están por concluir.

c) **Términos y condiciones de empleo:** como una condición del empleo, el personal debe estar claramente informado de sus responsabilidades de seguridad de la información. Los términos y las condiciones del empleo indican la responsabilidad de seguridad de la información del empleado, cuando es apropiado, estas responsabilidades continúan por un período definido después del término del empleo. Las responsabilidades legales y los derechos del empleado se deben clarificar e incluir dentro de los términos y condiciones del empleo, así como las acciones a tomar si el empleado desatiende los requerimientos de seguridad. La responsabilidad de clasificación y administración de los datos de la empresa se debe incluir siempre que sea apropiado, los términos y las condiciones del empleo indican que estas responsabilidades se extienden más allá de las instalaciones de la organización y de las horas normales de trabajo en caso de que éste se realice en el hogar.

d) **Capacitación:** un programa de capacitación en seguridad de la información se da a todos los empleados - incluyendo a los nuevos y a los ya establecidos. Para asegurarse de que los usuarios estén enterados de las amenazas y de las preocupaciones de seguridad de la información, y estén entrenados para apoyar la política de seguridad de la organización durante su trabajo normal; éstos deben entrenarse en procedimientos de seguridad y el uso correcto de los medios de procesamiento de la información para reducir al mínimo los riesgos posibles de seguridad. Es indispensable que todos los empleados de la organización y los usuarios externos reciban capacitación apropiada y actualizaciones regulares en políticas y procedimientos de la organización, esto incluye los requerimientos de seguridad, responsabilidades legales y controles del negocio, así como capacitación en el uso correcto de los medios de procesamiento de la información – procedimiento de conexión, uso de paquetes de software - antes de que se conceda el acceso a la información o a los servicios.

e) **Recurso:** un proceso formal para tratar con la violación de las políticas de seguridad de la información y responder a los incidentes y a los malos funcionamientos de la seguridad. Se busca reducir al mínimo, el daño de incidentes y de malos funcionamientos de la seguridad, supervisar y aprender de tales incidentes. Los incidentes observados o sospechosos que afectan la seguridad deben divulgarse lo más pronto posible, es importante que todos los empleados y contratistas se enteren de los procedimientos para reportar los diversos tipos de incidente – brechas en la seguridad, debilidades, amenazas o mal funcionamiento - que pueden tener un impacto en la seguridad de los activos de la organización.

Las siguientes políticas[16] son algunos ejemplos que sirven para esta cuarta sección, cabe aclarar que no son las únicas que existen:

- N° 090101 Preparación de los términos y condiciones del empleo: "Los términos y condiciones del empleo de la organización deben incluir requerimientos para cumplir con la seguridad de la información."

[16] Extraídas del documento The RUSecure™ Information Security Policies.

- N° 030905 Comunicación con los medios: "Sólo el personal autorizado puede hablar con los medios (periódicos, televisión, radio, revistas, etc.) acerca de problemas relacionados con la organización."

3.2.5 Seguridad física y ambiental

Los objetivos de esta sección son:

- Prevenir el acceso a la información de personas no autorizadas que pudieran ocasionar daños o interferencia.

- Prevenir la pérdida o daño en los activos que causarán interrupción en las actividades económicas.

- Prevenir el hurto y un mal uso de los recursos con información.

Los medios críticos o sensibles de procesamiento de información del negocio deben encontrarse en áreas seguras, protegidas por un perímetro definido de seguridad, con barreras de seguridad y controles apropiados de entrada, es importante que estas áreas estén protegidas físicamente contra el acceso no autorizado, el daño y la interferencia. La protección que se proporciona debe estar conmensurada con los riesgos identificados, además se recomienda una limpieza de escritorio y una política clara para reducir el riesgo de acceso no autorizado o el daño en documentos y medios de procesamiento de información.

Esta quinta sección trata al riesgo inherente de las propiedades de la organización e incluye[17]:

a) **Perímetro físico de la seguridad:** el perímetro de la seguridad de las propiedades debe ser físicamente sólido. Las propiedades pueden tener zonas múltiples basadas en un nivel de clasificación u otros requerimientos de la organización. La protección física puede lograrse creando varias barreras físicas alrededor de las instalaciones y de los medios de procesamiento de la información, cada barrera establece un perímetro de seguridad, cada uno

[17] Para información más detallada véase cada inciso en el Apéndice E.

incrementa la protección total que se proporciona. Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen los medios de procesamiento de la información. Un perímetro de seguridad es algo que construye una barrera - una pared, una puerta controlada por tarjeta o un escritorio de recepción -, la localización y la fuerza de cada barrera depende de los resultados de la evaluación de riesgo.

b) **Control de acceso:** las áreas seguras se deben proteger con controles apropiados de entrada para asegurarse de que solamente el personal autorizado tenga acceso.

c) **Equipo:** el equipo se debe localizar dentro de las instalaciones para asegurar la integridad y la disponibilidad físicas y ambientales. Además, se busca prevenir la pérdida, el daño o el compromiso de los activos y la interrupción a las actividades económicas. Siempre hay que proteger al equipo físicamente contra amenazas de seguridad y peligros del medio ambiente, la protección del equipo (incluyendo el que se encuentra fuera del lugar) es necesaria para reducir el riesgo del acceso no autorizado a los datos y protegerlos contra pérdida o daño, esto considera la localización y la disposición del equipo. Algunos controles especiales se requieren para proteger contra peligros o acceso no autorizado y para salvaguardar instalaciones, tales como la fuente eléctrica y la infraestructura de cableado.

d) **Transferencia de recursos:** mecanismos para lograr la entrada y salida de activos a través del perímetro de seguridad. Sin importar la pertenencia, el uso de cualquier equipo fuera de las instalaciones de una organización para el procesamiento de la información debe autorizarlo la administración.

e) **General:** deben existir políticas y estándares, como la utilización de fragmentos de equipo, almacenamiento seguro, principios de "limpieza de escritorio", para gobernar la seguridad operacional dentro del área de trabajo. Se busca prevenir el compromiso o el hurto de la información y de los medios de procesamiento de información, para ello, éstos se protegen de la divulgación, la modificación o el hurto por personas no autorizadas, y los controles se colocan en el lugar para reducir al mínimo la pérdida o el daño.

Las siguientes políticas[18] son algunos ejemplos que sirven para esta quinta sección, cabe aclarar que no son las únicas que existen:

- N° 010405 Cambio del hardware de un lugar a otro: "Cualquier movimiento de hardware de las instalaciones de la organización debe controlarse estrictamente mediante personal autorizado."

- N° 010201 Suministro de alimentación continua al equipo crítico: "Debe proveerse una fuente de alimentación continua para asegurar la continuidad de los servicios durante fallas de electricidad."

3.2.6 Gestión[19] de comunicaciones y operaciones

Los objetivos de esta sección son:

- Asegurar la operación correcta y segura de los recursos que realizan procesamiento de información.

- Reducir al mínimo el riesgo de fallas de los sistemas.

- Proteger la integridad lógica del software y de la información.

- Mantener la integridad y disponibilidad del procesamiento y de la comunicación de la información.

- Asegurar y salvaguardar la información en redes y la protección de la infraestructura que se utiliza.

- Prevenir las interrupciones de las actividades económicas y daños a los activos.

- Prevenir la pérdida, modificación o el mal uso de la información intercambiada entre las organizaciones.

- Establecer las responsabilidades y los procedimientos para la administración y la operación de todas las instalaciones de procesamiento de información.

[18] Extraídas del documento The RUSecure™ Information Security Policies.
[19] Acción y efecto de administrar.

Esta sexta sección trata la capacidad de una organización para asegurar la correcta y segura operación de sus recursos e incluye[20]:

a) **Procedimientos operacionales:** un amplio conjunto de procedimientos, en apoyo de los estándares y políticas de la organización. Los procedimientos de operación identificados por la política de seguridad deben documentarse y mantenerse, estos procedimientos de operación deben tratarse como documentos formales y cualquier cambio debe autorizarse por la administración.

b) **Control de cambios:** proceso para manejar el cambio y control de la configuración, incluyendo el manejo del cambio del sistema de administración de la seguridad de la información (SASI). Deben controlarse los cambios a las instalaciones y a los sistemas de procesamiento de la información. El control inadecuado de cambios a las instalaciones y a los sistemas de procesamiento de la información es una causa común de fallas del sistema o de la seguridad.

c) **Manejo de incidentes:** mecanismo para asegurar en tiempo y de manera efectiva una respuesta a cualquier incidente de seguridad. Las responsabilidades y los procedimientos de administración del incidente se establecen para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad.

d) **Separación de deberes:** separación y rotación de obligaciones para minimizar la posible confabulación y revelación descontrolada. La segregación de deberes es un método para reducir el riesgo de mal uso accidental o deliberado del sistema, es indispensable considerar la separación de la administración o ejecución de ciertos deberes o áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o mal uso de la información o de los servicios.

e) **Planificación de la capacidad:** mecanismo para supervisar y proyectar la capacidad de la organización para lograr que la disponibilidad no se interrumpa. Se busca reducir al mínimo el riesgo de las fallas de los sistemas. Se requieren el planeamiento y

[20] Para información más detallada véase cada inciso en el Apéndice F.

la preparación anticipados para asegurar la disponibilidad de la capacidad y de los recursos, por esto, se realizan proyecciones de los requerimientos futuros de capacidad para reducir el riesgo de la sobrecarga del sistema. Los requerimientos operacionales de sistemas nuevos se establecen, documentan y prueban antes de su aceptación y uso. Deben supervisarse las demandas de la capacidad y realizarse las proyecciones de los requerimientos futuros para asegurar que la energía adecuada de procesamiento y el almacenamiento estén disponibles. Es importante que estas proyecciones tomen en cuenta los nuevos requerimientos del negocio y del sistema, así como las tendencias actuales y proyectadas en el procesamiento de la información de la organización. Los mainframes requieren atención particular debido al costo y al tiempo, los encargados de los servicios del mainframe deben supervisar la utilización de los recursos claves del sistema, incluyendo procesadores, almacenamiento principal, almacenamiento de archivos, las impresoras, otros dispositivos de salida y los sistemas de comunicaciones, también deben identificar las tendencias en uso, particularmente en relación con las aplicaciones del negocio o el manejo de las herramientas del sistema de información. Los encargados deben utilizar esta información para identificar y para evitar los cuellos de botella potenciales que pueden presentar una amenaza a la seguridad o a los servicios del usuario del sistema y planear una acción remediadora apropiada.

f) **Aceptación del sistema:** metodología para evaluar los cambios del sistema y asegurar la continuidad de la confidencialidad, integridad y disponibilidad. Es necesario establecer criterios de aceptación para los nuevos sistemas de información, las mejoras y las nuevas versiones y realizar las pruebas convenientes del sistema antes de aceptarlos.

g) **Código malicioso:** controles para mitigar el riesgo debido a la introducción de código malicioso. Para proteger la integridad del software y de la información, se requieren precauciones para prevenir y para detectar la introducción de software malicioso. El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso, tal como virus de computadora, gusanos de red, caballos de Troya y bombas lógicas, es necesario que los usuarios estén enterados de los peligros

del software no autorizado o malicioso, y los encargados, cuando sea apropiado, introducir controles especiales para detectar o prevenir su introducción. En detalle, es esencial que se tomen precauciones para detectar y prevenir virus de computadora en las computadoras personales.

h) **Doméstico:** políticas, estándares, principios y procedimientos para manejar las actividades rutinarias como los respaldos de programas e inicios de sesión. Para mantener la integridad y la disponibilidad del procesamiento de información y los servicios de comunicación, es conveniente establecer procedimientos rutinarios para llevar a cabo la estrategia de respaldos acordada, para esto, se realizan respaldos de copias de datos y se ensaya su recuperación, eventos de conexión, averías y cuando sea apropiado, se supervisa el ambiente del equipo.

i) **Administración de red:** controles para manejar la operación segura de la infraestructura de la red. Se busca salvaguardar la información de las redes y la protección de la infraestructura de apoyo, es por esto, que la administración de la seguridad de las redes que pueden salir de los límites de la organización requiere atención.

j) **Manejo de medios:** controles para gobernar el manejo seguro y distribución segura de los medios de almacenamiento de la información y la documentación. Para prevenir el daño a los activos e interrupciones a las actividades económicas, los medios deben controlarse y protegerse físicamente.

k) **Intercambio de información:** controles para manejar el intercambio de información, incluyendo los acuerdos del usuario final, acuerdos del usuario y los mecanismos de transporte de la información. Se intenta prevenir la pérdida, la modificación o el mal uso de la información que se intercambia entre las organizaciones, para esto, los intercambios de información y de software entre las organizaciones deben controlarse y ser consistentes con cualquier legislación relevante. Es esencial que los intercambios se realicen con base en los acuerdos y que se establezcan procedimientos y estándares para proteger la información y los medios. Deben considerarse las implicaciones de negocio y de seguridad asociadas al intercambio de datos electrónicos, comercio electrónico y/o

correo electrónico y a los requerimientos para implementar controles.

Las siguientes políticas[21] son algunos ejemplos que sirven para esta sexta sección, cabe aclarar que no son las únicas que existen:

- N° 010204 Uso de Módems/ISDN/Conexiones DSL: "La información sensitiva o confidencial debe enviarse vía líneas telefónicas públicas sólo cuando no existan métodos seguros de transmisión. Tanto el dueño de la información y el receptor deben autorizar este tipo de transmisión."

- N° 010302 Uso de medios de almacenamiento removibles incluyendo discos y discos compactos: "Sólo el personal autorizado para instalar o modificar el software debe utilizar medios removibles para transferir datos a/desde la red de la organización. Cualquier otra persona debe requerir autorización."

3.2.7 Control de acceso

Los objetivos de esta sección son:

- Controlar el acceso a la información.
- Prevenir el acceso no autorizado a los sistemas de información.
- Asegurar la protección de servicios de red.
- Prevenir el acceso no autorizado a las computadoras.
- Detectar actividades no autorizadas.
- Asegurar la información al usar recursos móviles, la computadora y servicios de telecomunicaciones de una red.

Esta séptima sección trata la capacidad de la organización para controlar el acceso a los recursos, basándose en los requerimientos de seguridad y negocio, e incluye[22]:

[21] Extraídas del documento The RUSecure™ Information Security Policies.

a) **Requerimientos de negocio:** política que controla el acceso a los recursos de la organización con base en los requerimientos del negocio y "lo que necesita saber". Controla el acceso a la información, el acceso a ésta y los procesos de negocio deben controlarse con base en los requerimientos del negocio y de la seguridad, para esto, debe tomarse en cuenta las políticas para la difusión y la autorización de la información.

b) **Administración de usuario:** mecanismos para:

1. Registrar y eliminar el registro de usuarios.

2. Controlar y revisar accesos y privilegios.

3. Manejar contraseñas.

Se busca prevenir el acceso no autorizado a los sistemas de información, para esto, los procedimientos formales deben estar presentes para controlar la asignación de los derechos de acceso a los sistemas y servicios de información. Estos procedimientos deben cubrir todas las etapas del ciclo vital de acceso del usuario, desde el registro inicial de nuevos usuarios hasta la eliminación final del registro de los usuarios que no requieren más el acceso a los sistemas y servicios de información. Debe brindarse atención especial a la necesidad para controlar la asignación de derechos privilegiados de acceso, que permiten que los usuarios contrarresten los controles del sistema.

c) **Responsabilidades del usuario:** informar a los usuarios de sus responsabilidades de control de acceso, incluyendo posesión de contraseña y equipo descuidado. Se previene el acceso del usuario no autorizado, la cooperación de usuarios autorizados es esencial para la seguridad eficaz, ya que los usuarios deben enterarse de sus responsabilidades para mantener los controles de acceso eficaces, particularmente con respecto al uso de contraseñas y a la seguridad del equipo del usuario.

[22] Para información más detallada véase cada inciso en el Apéndice G.

d) **Control de acceso en la red:** es la protección de servicios en red ya que se refiere a la política sobre el uso de los servicios de red, incluyendo mecanismos para:

1. Autenticar nodos.
2. Autenticar usuarios externos.
3. Definir ruta.
4. Controlar la seguridad de los dispositivos de red.
5. Mantener la separación o segmentación de la red.
6. Controlar las conexiones de red.
7. Mantener la seguridad de los servicios de seguridad.

Es la protección de servicios en red.

e) **Control de acceso del sistema operativo:** mecanismos para:

1. Inicio de sesión segura.
2. Identificar automáticamente terminales.
3. Autenticar usuarios.
4. Manejar contraseñas.
5. Asegurar utilidades del sistema.
6. Suministrar a los usuarios emergencias contra el encierro como "botones de pánico".
7. Habilitar tiempos de espera de terminal, usuario o conexión.

Se intenta prevenir el acceso no autorizado a la computadora.

f) **Aplicación del control de acceso:** limita el acceso a las aplicaciones con base en el usuario o en los niveles de autorización.

Previene el acceso no autorizado a la información almacenada en los sistemas de información, es conveniente que las instalaciones o medios de seguridad se utilicen para restringir el acceso dentro de las aplicaciones del sistema. El acceso lógico al software y a la información se debe restringir sólo a los usuarios autorizados.

g) **Supervisión de acceso:** mecanismos para supervisar el acceso al sistema y el uso del sistema para detectar actividades no autorizadas. El sistema debe supervisarse para detectar la desviación de la política de control de acceso y registrar acontecimientos que proporcionen evidencia en caso de incidentes de seguridad. La supervisión del sistema permite la eficacia de los controles adoptados para ser comprobados y consistentes con un modelo de política de acceso.

h) **Cómputo móvil:** políticas y estándares para tratar la protección del activo, el acceso seguro, y responsabilidades del usuario. Se busca lograr la seguridad de la información cuando se utiliza el cómputo móvil y las telecomunicaciones, la protección que se requiere debe estar conmensurada con los riesgos que estas maneras específicas de trabajar causa. Cuando se utiliza el cómputo móvil, deben considerarse los riesgos de trabajo en un ambiente desprotegido y es importante que se aplique una protección apropiada. En el caso de las telecomunicaciones, la organización debe aplicar protección en el sitio de telecomunicaciones y asegurarse de que existan las acciones convenientes dentro del lugar para su correcto desempeño.

Las siguientes políticas[23] son algunos ejemplos que sirven para esta séptima sección, cabe aclarar que no son las únicas que existen:

- N° 020101 Manejo de estándares de control de acceso: "La administración debe establecer los estándares de control de acceso a los sistemas de información y debe prevenir el acceso no autorizado aun cuando se permita el acceso libre para alcanzar las necesidades de negocio."

- N° 010402 Expedición de laptops y/o computadoras portátiles al personal: "La administración debe autorizar la expedición de computadoras portátiles. Su uso se restringe a propósitos del negocio

[23] Extraídas del documento The RUSecure™ Information Security Policies.

y debe avisarse a los usuarios para que acepten los términos y condiciones de uso y principalmente la responsabilidad para mantener la seguridad de la información."

3.2.8 Desarrollo y mantenimiento de sistemas

Los objetivos de esta sección son:

- Asegurar la construcción de sistemas operacionales.
- Prevenir la pérdida, modificación o mal uso de los datos en sistemas o aplicaciones.
- Mantener la confidencialidad, la autenticidad y la integridad de la información.
- Asegurar que los proyectos y las actividades de ayuda se conduzcan de una manera correcta.
- Mantener la seguridad del software del sistema y de los datos de la aplicación.

Esta octava sección trata la capacidad de la organización para asegurar que los controles apropiados de la seguridad del sistema de información se incorporen y se mantengan, e incluye[24]:

a) **Requerimientos de seguridad del sistema:** incorpora las consideraciones de la seguridad de la información en las especificaciones de cualquier desarrollo o consecución del sistema, para asegurarse de que la seguridad exista en los sistemas de información, esto incluye la infraestructura, aplicaciones de negocio y aplicaciones de usuario y desarrollo. El diseño y la implementación del proceso de negocio que soporta la aplicación o el servicio son cruciales para la seguridad, ya que los requerimientos de seguridad se deben identificar y convenir antes del desarrollo de los sistemas de información. Todos los requerimientos de seguridad, se deben identificar en la fase de requerimientos de un proyecto y

[24] Para información más detallada véase cada inciso en el Apéndice H.

justificar, convenir y documentar como parte del negocio para un sistema de información.

b) **Requerimientos de la seguridad de la aplicación:** incorpora las consideraciones de la seguridad de la información en la especificación de cualquier desarrollo o consecución de la aplicación. Sirve para prevenir la pérdida, la modificación o el mal uso de los datos del usuario en los sistemas de aplicación, para esto, controles apropiados y registros de actividad deben diseñarse dentro de los sistemas de aplicación, incluyendo las aplicaciones escritas por el usuario. Tales sistemas deben incluir la validación de los datos de entrada, del proceso interno y de los datos de la salida. Pueden requerirse controles adicionales para los sistemas que procesan, o tienen un impacto en los activos sensibles, valiosos o críticos de la organización, tales controles deben determinarse con base en los requerimientos de seguridad y la evaluación de riesgo.

c) **Criptografía:** políticas, estándares y procedimientos que gobiernan el uso y el mantenimiento de controles criptográficos. Se busca proteger la confidencialidad, la autenticidad o la integridad de la información, esto se logra utilizando sistemas y técnicas criptográficas para proteger la información que se considera en riesgo y para la cual otros controles no proporcionan la protección adecuada.

d) **Integridad del sistema:** mecanismos para controlar el acceso y verificar la integridad del software operacional y los datos, incluyendo un proceso para rastrear, evaluar e incorporar actualizaciones y parches a los activos. Para lograr que los proyectos de tecnología de información y las actividades de apoyo se conduzcan de una manera segura, debe controlarse el acceso a los archivos del sistema. Mantener la integridad del sistema debe ser responsabilidad del usuario o del grupo de desarrollo a los cuales el sistema o el software de aplicación pertenece.

e) **Seguridad en el desarrollo:** integra control de cambio y revisiones técnicas en el proceso de desarrollo. Para mantener la seguridad del software de aplicación del sistema y de la información, los ambientes del proyecto y de apoyo deben controlarse estrictamente. Los administradores responsables de los sistemas de aplicación

también deben ser responsables de la seguridad del proyecto o el ambiente de apoyo, ya que deben asegurarse de que todos los cambios propuestos al sistema se revisen para comprobar que no comprometen la seguridad del sistema o del ambiente de funcionamiento.

Las siguientes políticas[25] son algunos ejemplos que sirven para esta octava sección, cabe aclarar que no son las únicas que existen:

- N° 030205 Manejo de claves electrónicas: "La administración de claves electrónicas para controlar tanto el cifrado como el descifrado de mensajes sensitivos debe ejecutarse bajo un control dual, con deberes que se alternarán entre el personal."

- N° 030214 Administración o uso de la transacción y/o procesamiento de reportes: "La transacción y el procesamiento de reportes deben revisarse regularmente por un personal calificado y capacitado."

3.2.9 Plan de continuidad del negocio

El objetivo de esta sección es:

- Evitar interrupciones a las actividades económicas y a los procesos críticos del negocio, evaluando los efectos de incidentes o de desastres importantes.

Esta novena sección trata la capacidad de una organización para contrarrestar interrupciones a las operaciones normales, e incluye[26]:

a) **Planeamiento de la continuidad del negocio:** estrategia de la continuidad del negocio basada en un análisis del impacto del negocio. Para contrarrestar las interrupciones a las actividades del negocio y proteger sus procesos críticos del negocio contra los efectos de fallas o de desastres importantes, debe implementarse un proceso de administración de la continuidad del negocio, ya que se busca reducir la interrupción causada por desastres y fallas de seguridad (las cuales pueden ser el resultado, por ejemplo, de

[25] Extraídas del documento The RUSecure™ Information Security Policies.
[26] Para información más detallada véase cada inciso en el Apéndice I.

desastres naturales, accidentes, fallas en el equipo, y acciones deliberadas) a un nivel aceptable mediante la combinación de controles preventivos y de recuperación. Deben analizarse las consecuencias de desastres, fallas de seguridad y la pérdida de servicio y desarrollarse e implementarse planes de contingencia para asegurar que los procesos del negocio se pueden restaurar dentro del período de tiempo requerido. Deben mantenerse y practicarse tales planes para convertirlos en una parte integral de todos los procesos de administración, la administración de continuidad del negocio debe incluir controles para identificar y reducir riesgos, para limitar las consecuencias de incidentes dañinos y asegurar la reanudación oportuna de las operaciones esenciales.

b) **Prueba de la continuidad del negocio:** prueba y documentación de la estrategia de la continuidad del negocio. Los planes de continuidad del negocio pueden fallar en la prueba debido a suposiciones, descuidos, o cambios incorrectos en el equipo o el personal, por lo tanto, deben probarse regularmente para asegurar que son actuales y eficaces. Es esencial que tales pruebas también aseguren que los miembros del equipo de recuperación y otro personal relevante se enteren de los planes. El horario de prueba para los planes de continuidad del negocio debe indicar cómo y cuándo probar cada elemento del plan, se recomienda probar los componentes individuales del plan con frecuencia.

c) **Mantenimiento de la continuidad del negocio:** identifica la propiedad de la estrategia de continuidad del negocio así como la nueva (o revaloración) evaluación y el mantenimiento en curso. Los planes de continuidad del negocio deben mantenerse mediante revisiones y actualizaciones regulares para asegurar su eficacia de continuación. Los procedimientos deben incluirse dentro del programa de administración del cambio de la organización para asegurar que los asuntos de continuidad del negocio se tratan apropiadamente, es importante también asignar responsabilidades para realizar revisiones regulares de cada plan de continuidad del negocio; la identificación de cambios en las acciones del negocio no reflejados en los planes de continuidad, debe seguirse mediante una actualización apropiada del plan. Este proceso formal de control del cambio debe asegurar que los planes actualizados se distribuyan y refuercen mediante revisiones regulares del plan completo.

Las siguientes políticas[27] son algunos ejemplos que sirven para esta novena sección, cabe aclarar que no son las únicas que existen:

- N° 060102 Minimizando el impacto de los ataques cibernéticos: "Deben prepararse, mantenerse y regularmente probarse planes para asegurar que el daño provocado por posibles ataques cibernéticos externos se minimice y que se realice la restauración lo más pronto posible."

- N° 080103 Desarrollo del plan de continuidad del negocio: "La administración debe desarrollar un plan de continuidad del negocio que cubra todas las actividades críticas y esenciales del negocio."

3.2.10 Cumplimiento

Los objetivos de esta sección son:

- Evitar la ambigüedad de cualquier obligación criminal o civil, estatutos reguladores o contractuales que tengan relación con cualquier requisito de seguridad.

- Asegurar la conformidad entre sistemas de seguridad y políticas o estándares de la organización.

- Maximizar la eficacia y reducir al mínimo la interferencia externa a los procesos o sistemas.

Esta última sección trata la capacidad de la organización para permanecer en conformidad con los requerimientos reguladores, estatutarios[28], contractuales y de seguridad, e incluye[29]:

a) Requerimientos legales: conocimiento de:

1. Legislación apropiada.

2. Derechos de propiedad intelectual.

---

[27] Extraídas del documento The RUSecure™ Information Security Policies.
[28] Conforme a las disposiciones o reglas legales.
[29] Para información más detallada véase cada inciso en el Apéndice J.

3. Salvaguardia de registros administrativos.

4. Privacidad de datos.

5. Prevención de abuso.

6. Regulación de criptografía.

7. Recopilación de evidencia.

Se trata de evitar las brechas en cualquier ley criminal, civil, u obligaciones estatutarias, reguladoras o contractuales y de cualquier requerimiento de seguridad.

b) Requerimientos técnicos: mecanismo para verificar la ejecución e implementación de las políticas de seguridad y el cumplimiento técnico. Para asegurar el cumplimiento de los sistemas con políticas y estándares de seguridad de la organización, la seguridad de los sistemas de información debe revisarse regularmente, tales revisiones deben realizarse en comparación con las políticas apropiadas de seguridad y las plataformas técnicas; deben revisarse los sistemas de información para mantener el cumplimiento con los estándares de implementación de seguridad.

c) Revisiones del sistema: controles de revisión para maximizar la eficacia, minimizar la desorganización y proteger las herramientas de revisión. Para maximizar la eficacia y para reducir al mínimo la interferencia a/del proceso de revisión del sistema, es indispensable la existencia de controles para salvaguardar sistemas operacionales y herramientas de verificación durante la inspección del sistema, es vital considerar protección para salvaguardar la integridad y para prevenir el mal uso de las herramientas de verificación.

Las siguientes políticas[30] son algunos ejemplos que sirven para esta décima sección, cabe aclarar que no son las únicas que existen:

- N° 090205 Divulgación de información del empleado con otros empleados: "Los datos del empleado sólo debe divulgarse a personas específicamente autorizadas para recibir esta información."

[30] Extraídas del documento The RUSecure™ Information Security Policies.

- N° 090317 Uso de juegos en las computadoras de la oficina: "Está prohibido el uso de juegos en computadoras personales o laptops de la oficina."

CAPÍTULO 4

APLICACIÓN DEL ESTÁNDAR ISO 17799

4.1 Proceso

El proceso para implementar la administración de la seguridad de la información haciendo uso del estándar ISO 17799, se muestra en la figura 4.1.

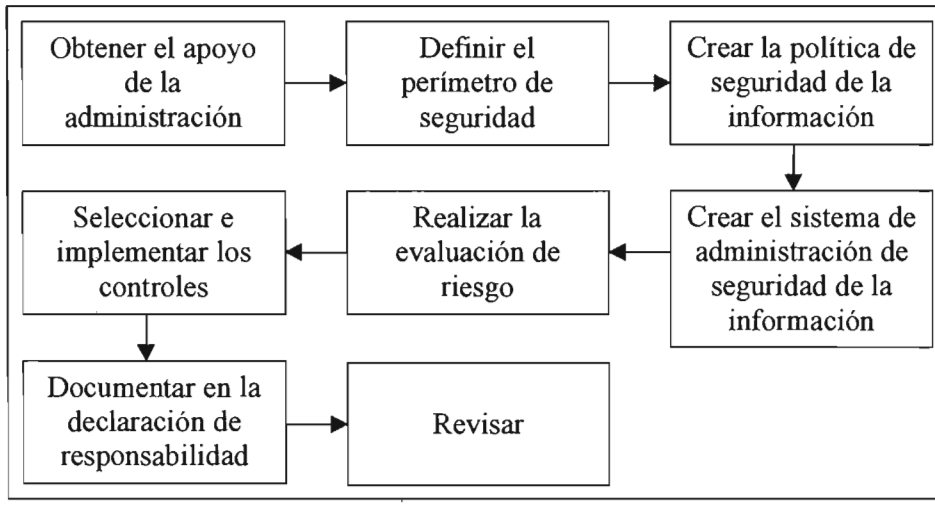

Figura 4.1. Proceso del estándar ISO 17799

Como se observa, este proceso consta de ocho pasos y éstos se describen a continuación:

1. Obtener el apoyo de la administración superior

   La componente crucial para lograr el éxito de un programa que permita adoptar el estándar ISO 17799 es ganar el apoyo de la administración superior. El proceso para establecer una infraestructura complaciente puede ser costoso, y el entusiasmo y el esmero pueden decaer con el tiempo, sin embargo, una implementación acertada del estándar ISO 17799 inculca la seguridad como una forma de vida de la organización que se maneja desde el nivel más alto. La seguridad de la información no es un programa; es un proceso.

2. Definir el perímetro de seguridad

Una de las tareas iniciales más difíciles es definir el perímetro de seguridad o el dominio de seguridad, en el cual se va a adoptar el estándar ISO 17799. El perímetro de seguridad puede o no abarcar a toda la organización; sin embargo, el perímetro de seguridad debe estar bajo el control de una sola organización, ya que si una organización no puede controlarlo, no podrá manejarlo con eficacia.

3. Crear la política de seguridad de la información

Las políticas de seguridad de la información pueden tomar múltiples formas, puesto que es posible que se contengan en un documento de políticas, documentos múltiples adaptados a diversas audiencias o declaraciones de política incorporadas dentro de estándares. Sin embargo, el objetivo es el mismo: una declaración de alto nivel de implementación independiente que demuestra el apoyo de la administración superior a los conceptos y a las metas de la seguridad de la información.

4. Crear el sistema de administración de seguridad de la información

Se debe crear un marco - sistema de administración de la seguridad de la información (SASI) - para implementar, manejar, mantener y hacer cumplir el proceso de seguridad de la información. Éste debe establecerse y autorizarse con el apoyo de la administración superior y evidenciarse en la política de seguridad de la información. El SASI define el perímetro de seguridad y proporciona el mapa que detalla las estrategias de seguridad de la información para cada una de las diez secciones de control del estándar ISO 17799. Estas estrategias pueden utilizarse para la creación de políticas, estándares, procedimientos, planes, comités, y equipos o para emplear a personal específico. Es importante que al inicio del proceso de creación del SASI se identifique y autorice a un guía de seguridad o a un oficial de seguridad del sistema de información para coordinar, supervisar, y adueñarse, en última instancia, del SASI.

5. Realizar la evaluación de riesgo

El estándar ISO 17799 se trata de la administración del riesgo. Se implanta desarrollando una administración de riesgo y una estrategia de mitigación por medio de la cual se identifican los activos, las amenazas, las vulnerabilidades y se cuantifica el riesgo conmensurado. Se pueden entonces seleccionar los controles para evitar, transferir, o reducir el riesgo a un nivel aceptable. La evaluación de riesgo de la seguridad es un método para maximizar el uso de los activos finitos de la organización basados en el riesgo mensurable y la tolerancia de riesgo de la organización. Los pasos de la evaluación de riesgo son los siguientes:

a) **Identificar los activos dentro del perímetro de seguridad:** un activo puede ser un artículo tangible, tal como el equipo, o intangible, tal como una base de datos de la organización. Por definición, un activo tiene valor para la organización, por lo tanto, requiere protección. Los activos deben identificarse y es indispensable determinar a los propietarios. Un valor relativo también debe establecerse para cada activo, de tal forma que la importancia puede implantarse cuando se cuantifiquen los riesgos.

b) **Identificar las amenazas a los activos:** las amenazas explotan o se aprovechan de las vulnerabilidades del activo para ocasionar daños. Para cada activo deben identificarse las amenazas, sin embargo, pueden existir múltiples amenazas para cada uno. La identificación de éstas debe ser real, es decir, deben considerarse solamente aquéllas que tienen una probabilidad significativa o daño extremo. Por ejemplo, una amenaza a la base de datos de la organización puede ser hurto o alteración.

c) **Identificar las vulnerabilidades de los activos:** las vulnerabilidades son deficiencias reconocidas en los activos que se pueden explotar mediante amenazas y crear riesgos. Un activo puede tener múltiples vulnerabilidades, por ejemplo, la vulnerabilidad de la base de datos de una organización puede ser un control de acceso pobre o respaldos escasos.

d) **Determinar la probabilidad real:** deben determinarse las probabilidades para cada combinación de amenaza/vulnerabilidad.

Las combinaciones con probabilidad estadística insignificante pueden omitirse.

e) **Calcular el daño:** el daño (designado a veces como impacto) se puede cuantificar numéricamente para reflejar el daño de un ataque exitoso. Este valor permite la clasificación independiente de la seriedad de un riesgo con base en una escala relativa de acuerdo a su probabilidad.

f) **Calcular el riesgo:** la evaluación y la mitigación del riesgo es la meta del SASI del estándar ISO 17799. Matemáticamente, el riesgo se puede expresar como: Probabilidad x Daño. Este cálculo da lugar a una clasificación numérica del riesgo basado en el activo para un sistema dado de amenazas y de vulnerabilidades. Esta interpretación numérica permite dar prioridad a los recursos finitos de la mitigación del riesgo. Es importante hacer notar que la eficacia del proceso del estándar ISO 17799 se basa en la exactitud y la minuciosidad de la evaluación de riesgo de la seguridad. El riesgo no se puede atenuar si no se identifica.

6. Seleccionar e implementar los controles

Los controles atenúan los riesgos identificados en la evaluación de riesgo de seguridad. La selección de controles se basa en la disponibilidad de activos y la capacidad de la administración para aceptar ciertos riesgos en lugar de implementar controles. Esto puede decidirse según el valor del riesgo identificado en el paso 5.

7. Documentar en la declaración de responsabilidad

Una declaración de responsabilidad es la porción del SASI que documenta cómo los riesgos identificados en la evaluación de riesgo de la seguridad son mitigados por la selección de controles, este documento trata las diez secciones de control de la ISO 17799 y tabula la selección o la ausencia de controles junto con el análisis realizado según lo requerido. Mientras que el SASI dice qué van a hacer las organizaciones, la declaración de responsabilidad es donde las organizaciones documentan si el responsable hizo lo que dijo que haría.

8. Revisar

La revisión permite la verificación de la implementación de la infraestructura de seguridad de la información. Las revisiones pueden ser de tres tipos:

a) Primera entidad: una organización realiza la revisión por sí misma.

b) Segunda entidad: un cliente o socio realiza la revisión.

c) Tercera entidad: un verificador independiente realiza la revisión.

Es indispensable la revisión de tercera entidad para lograr la certificación de cumplimiento.

4.2 Estructura de la organización de la seguridad

La figura 4.2 es un ejemplo de una estructura de la organización de la seguridad que resulta de la aplicación del proceso del estándar ISO 17799.

En esta estructura de la organización de la seguridad se observa:

1. Declaración de la política de seguridad

La declaración de la política de seguridad es una declaración de propósito general a nivel superior para la administración superior, es similar a una "declaración de la misión" orientada a la seguridad. Su intento es demostrar el compromiso de la administración superior con las metas de seguridad de la información y por lo tanto, autoriza la estructura de la organización de la seguridad. La declaración de la política de seguridad incluye declaraciones de tal manera que la política de la organización sea la que:

a) Asegure la confidencialidad de la información.

b) Mantiene la integridad de la información.

c) Garantice la disponibilidad de la información que los usuarios autorizados necesiten.

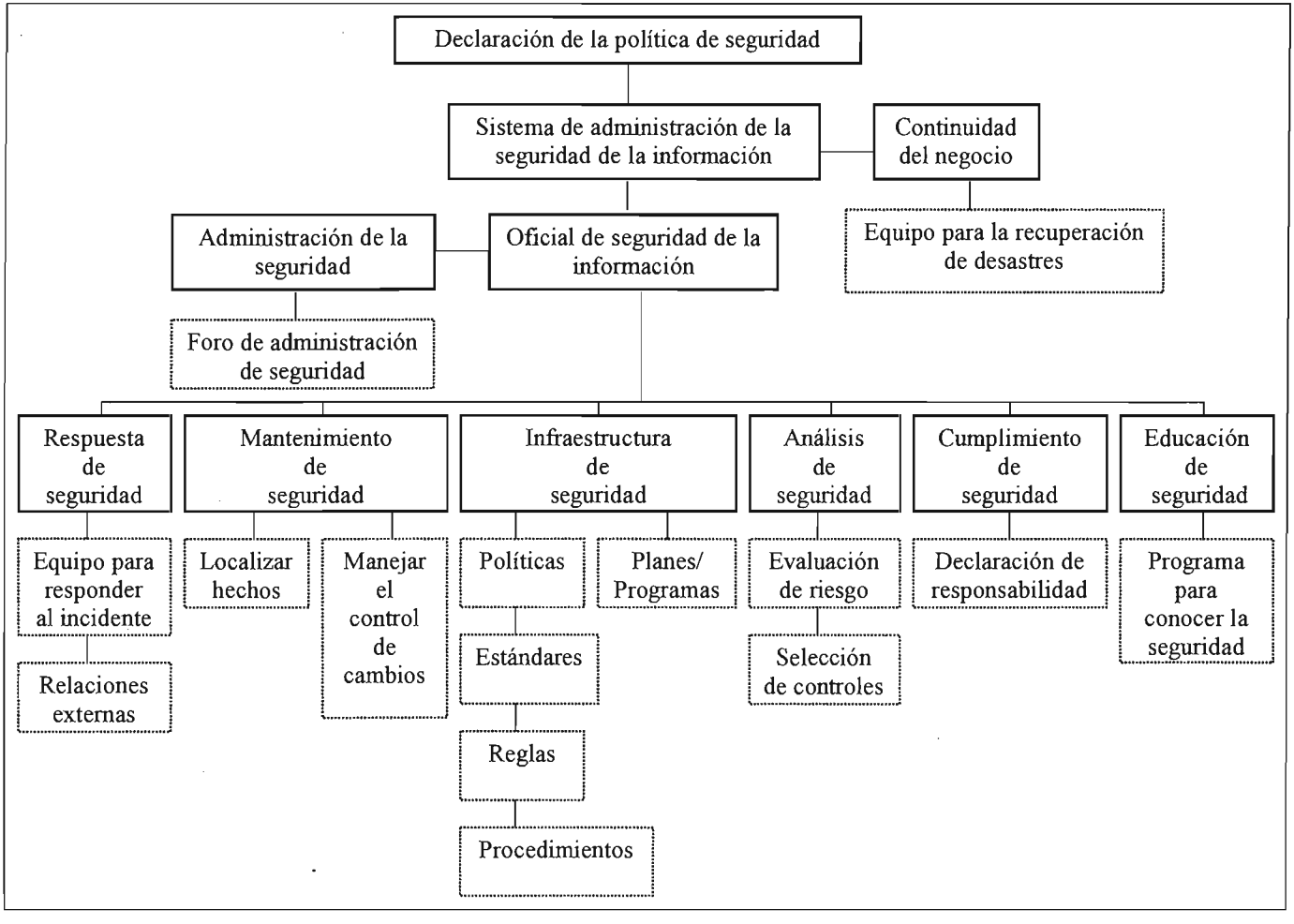

Figura 4.2. Estructura de la organización de la seguridad

d) Verifique los requerimientos reguladores y legislativos.

e) Asegure que la capacitación en seguridad de la información esté disponible para todo el personal.

f) Las brechas en la seguridad de la información, reales o sospechosas, serán divulgadas, e investigadas por el oficial de seguridad del sistema de información.

La naturaleza no específica de la declaración de la política de seguridad la hace apropiada para el acceso público.

2. Sistema de administración de la seguridad de la información (SASI)

El SASI es la estrategia de administración de riesgo de la organización, se establece y autoriza mediante la declaración de la política de seguridad y lo maneja el oficial de seguridad del sistema de información. Dentro del SASI, se define el perímetro de seguridad, se tratan las diez secciones de control del estándar ISO 17799 y una estrategia de administración de riesgo se detalla para cada sección de control. El SASI también sirve como referencia para la documentación externa de apoyo que correlaciona la documentación de la administración de riesgo con las diez secciones de control del estándar. SASI es un mapa de seguridad de la información específica de la organización. La documentación del SASI incluye:

a) Diagrama de la organización de la estructura de la seguridad.

b) Estrategia de la administración del riesgo.

c) Descripción de las funciones del oficial de seguridad del sistema de información.

d) Certificado del foro de administración de seguridad.

e) Documento del plan de control del SASI.

f) Evaluación del riesgo de seguridad.

g) Declaración de responsabilidad.

h) Código de conducta del cliente.

i) Documento matriz del estándar ISO 17799 que enumera todos los documentos aplicables.

j) Dibujos de la demarcación del perímetro de seguridad.

3. Continuidad del negocio

a) Plan de continuidad de las actividades: un análisis del impacto de la organización que produce un plan comprensivo de la continuidad de las actividades, especifica la pertenencia y un calendario de revisión.

b) Equipo para la recuperación de desastres: es el medio para probar e implementar el plan de continuidad del negocio.

4. Oficial de seguridad de la información

Debe identificarse, designarse, y autorizarse un oficial de seguridad del sistema de información. Una descripción formal de las funciones define los deberes principales del oficial de seguridad del sistema de información, que incluyen:

a) Conducir el foro de administración de seguridad.

b) Conducir al equipo para responder al incidente.

c) Preparar los informes de seguridad del foro de administración de seguridad.

d) Registrar y resolver los incidentes de seguridad.

e) Mantener el SASI.

f) Establecer y revisar la evaluación de riesgo de la seguridad.

g) Seleccionar los controles y la mitigación del riesgo.

h) Mantener la declaración de la responsabilidad.

i) Supervisar la conformidad en curso con estándares de seguridad.

j) Establecer y mantener contactos con los recursos externos de seguridad.

k) Evaluar los cambios con base en el activo e implicaciones resultantes de la seguridad.

l) Consultar y aconsejar sobre ediciones de seguridad de la información de carácter general.

5. Administración de la seguridad

El foro de administración de la seguridad se encuentra formado por el oficial principal de información, el administrador de ingeniería, el administrador del centro de datos y el oficial de seguridad del sistema de información. Otros miembros se incluyen según se requiera. Los deberes del foro de administración de la seguridad son:

a) Proporcionar ayuda a la administración en curso en el proceso de seguridad.

b) Servir como canal alternativo para la discusión de las ediciones de seguridad.

c) Desarrollar objetivos, estrategias, y políticas de seguridad.

d) Discutir el estado de las iniciativas de seguridad.

e) Obtener y revisar los informes de seguridad del oficial de seguridad del sistema de información.

f) Revisar los informes y las resoluciones de incidentes de la seguridad.

g) Formular los umbrales de la administración de riesgo y los requisitos del aseguramiento.

h) Revisión y aprobación anual de la política de seguridad de la información.

i) Revisión y aprobación anuales del SASI.

6. Respuesta de seguridad

a) Equipo para responder a incidentes: formado para crear y realizar un plan de respuesta a incidentes. El equipo debe incluir conjuntos diversos de capacidades que cubren todos los aspectos de los sistemas de procesamiento de la información de una organización. Se obtienen las herramientas, se capacita a los miembros y se determinan los roles. El equipo se establece con la misión de respuesta del incidente para:

- Prepararse para un incidente.
- Identificar un incidente.
- Reprimir el incidente.
- Erradicar al intruso.
- Recuperarse de la intrusión.
- Aprender del incidente.

Las metodologías incluyen procesos para:

- Identificar y medir los acontecimientos de seguridad.
- Determinar la seguridad de la organización.
- Mantener la seguridad de la organización.

b) Relaciones externas: establecidas con las agencias locales que aplican la ley, así como con entidades que manejan las relaciones legales y públicas.

7. Mantenimiento de seguridad

   a) **Localizar hechos:** los especialistas calificados en diversos elementos de la red de una organización señalan la localización de ataques relevantes y reportan información preocupante al oficial de seguridad del sistema de información.

   b) **Manejar el control de cambios:** proceso autorizado para manejar el cambio. El proceso de control de cambio incluye la petición para someterse al cambio y la evaluación, así como procedimientos de recuperación y retroceso. Además, un plan de control del documento se realiza para controlar la documentación del SASI.

8. Infraestructura de seguridad

   a) **Políticas:** expresan las metas conceptuales de seguridad de la información de la organización en la política de seguridad de la información.

   b) **Estándares:** apoyan la implementación de la política de seguridad de la información. Los estándares pueden tratar:

      - Seguridad del personal.
      - Conducta del empleado.
      - Clasificación de los datos.
      - Etiquetado de los datos.
      - Manejo de los datos.
      - Transmisión de datos.
      - Cifrado de datos.
      - Redes privadas virtuales.

- Recuperación de los datos.
- Encaminamiento de los datos.
- Control de acceso.
- Estándar de firewall.
- Seguridad de la red.
- Aplicación de la red.
- Conmutación de los datos.
- Registro.
- Administración del activo.
- Alarma.
- Seguridad física.
- Mantenimiento de la seguridad.

c) **Reglas:** formalizan la adopción de las mejores prácticas de seguridad de la información. Las pautas pueden tratar:

- Control de acceso.
- Protección de los datos.
- Configuración del encaminador.
- Seguridad de la organización.

d) **Procedimientos:** detallan la implementación de la seguridad de la información con ayuda de estándares y políticas relevantes. Los procedimientos pueden tratar:

- Administración de riesgo.
- Respaldo/Restauración.
- Añadir/borrar/modificar un usuario del sistema.
- Aprovisionamiento del cliente.
- Mantenimiento de equipo.
- Control del activo.
- Alarma.
- Mantenimiento de la seguridad.
- Añadir/borrar/modificar una terminal del servidor.
- Cambio secreto de la contraseña/cuota.
- Disposición del firewall.
- Respuesta al incidente.

e) **Planes/Programas:** satisfacen metas de seguridad de la información. Los planes y los programas pueden tratar:

- Conocimiento de la seguridad de la información.
- Control de cambio.
- Respuesta al incidente.
- Detección de la intrusión.
- Continuidad del negocio.
- Prueba de aceptación.

9. Análisis de seguridad

a) **Evaluación de riesgo de seguridad:** identifica los activos relevantes, amenazas, y vulnerabilidades. La evaluación de riesgo de seguridad se revisa en un calendario fijado por el oficial de seguridad del sistema de información.

b) **Selección de los controles:** se seleccionan con base en el grado de riesgo, la disponibilidad de los activos de mitigación del riesgo, y la determinación de la administración para aceptar riesgos residuales.

10. Cumplimiento de seguridad

Una declaración de responsabilidad trata las diez secciones de control del estándar ISO 17799, detallando cómo los riesgos identificados en la evaluación de riesgo de la seguridad se atenuaron vía la selección de controles o fueron aceptados. Debido a la naturaleza amplia y general del estándar ISO 17799, no todas las secciones de control son aplicables a cada organización, además, la administración puede decidir que la aceptación de algunos riesgos es preferible al costo de mitigación. La declaración de responsabilidad está donde las decisiones de seguridad se racionalizan y se documentan, ésta documenta las obligaciones y la toma racional de decisiones.

11. Educación de seguridad

a) **Programa para conocer la seguridad:** el personal debe tener el conocimiento para entender el significado de sus acciones. La interacción humana puede actuar de maneras que minan los controles de seguridad, causando aberturas en la seguridad. Se establece un programa de conocimiento de la seguridad para:

- Clarificar por qué la seguridad es importante y los controles son necesarios.
- Clarificar las responsabilidades de la seguridad del empleado.
- Servir como un foro para discutir preguntas de seguridad.

El programa de conocimiento de la seguridad debe incluir orientación sobre nuevos contratos o posibles sobornos y actividades en curso de actualización.

CONCLUSIONES

Sabiendo que una empresa certificada bajo un estándar internacional de seguridad de la información puede administrar ésta con eficiencia y efectividad, reduciendo vulnerabilidades y teniendo un mejor manejo de los riesgos, con este trabajo se le proporciona al lector un libro de texto que servirá de base para adentrarse en el mundo de la gestión de la seguridad e implementarla en cualquier organización que lo requiera, esto es, debido a que un proceso de certificación con base en un estándar asegura a los clientes y asociados que la información distribuida o guardada en las redes empresariales está segura y que la seguridad general de la organización es confiable.

Lograr la certificación es un factor de competitividad y posición en el mercado, ya que le permite a las empresas certificadas tener mejores relaciones en el extranjero, aunado a que la organización se mantendrá actualizada en las últimas vulnerabilidades y mejores procedimientos de la seguridad mediante auditorías y revisiones externas continuas y que la reducción de las vulnerabilidades significará menores transgresiones a la seguridad, lo cual generará una disminución de los fraudes, de los riesgos financieros y jurídicos, logrando así ahorro de tiempo, credibilidad en la información y la confianza de los clientes.

Este trabajo al ser uno de los primeros en el país y en el idioma español que trata este tema a profundidad, puede ser utilizado como base para implementar la gestión de la seguridad de la información en cualquier organización, así como guía para futuras investigaciones y desarrollo de aplicaciones en esta área que tanto bien harían a nuestro país.

Para algunas organizaciones incluso aquéllas que requieren altos grados de seguridad y confianza, la certificación ISO 17799 debería ser obligatoria, aunque para otras, la certificación sea una herramienta de mercado, esto se debe a que una empresa certificada con el estándar ISO 17799 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa certificada.

Si alguna organización no ha adoptado un programa de protección definido de la información, este trabajo puede servir de parámetro para que lo defina. Incluso si se decide a no ser certificado, servirá de guía para configurar la política de seguridad de la organización. En todo caso, debe tenerse en cuenta que ISO 17799 es un buen esquema de seguridad que la empresa puede

adoptar, pues es conveniente tener una guía reconocida internacionalmente para lograr una gran competitividad a nivel mundial.

Tomando en cuenta que alinearse con el estándar ISO17799 no es una tarea fácil, incluso para las organizaciones con más conciencia en la seguridad, se recomienda que el estándar se implemente bajo un esquema paso a paso, puesto que el mejor punto de partida es realizar un análisis de la posición y situación de la organización, seguido de una identificación de los cambios necesarios para alinearse con el estándar ISO 17799. A partir de este punto, los procesos de planeación e implementación deben realizarse metódicamente y siempre permanecer abiertos al cambio.

APÉNDICE A

POLÍTICA DE SEGURIDAD

a) **Documento de la política de seguridad de la información:** Como mínimo, los siguientes puntos deben incluirse:

1. Una definición de la seguridad de la información, sus objetivos, alcance y la importancia de la seguridad como un mecanismo habilitado para el intercambio de información.

2. Una declaración del propósito de la administración, sustentando las metas y principios de seguridad de la información.

3. Una breve explicación de la política de seguridad, principios, estándares y requerimientos de cumplimiento que son de importancia para la organización, por ejemplo:

   - Cumplimiento con requerimientos legislativos y de contrato.
   - Requerimientos de educación de seguridad.
   - Prevención y detección de virus y otro software malicioso.
   - Manejo de la continuidad del negocio.
   - Consecuencias de las violaciones a la política de seguridad.

4. Una definición de las responsabilidades generales y específicas para el manejo de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad.

5. Referencias a la documentación, la cual debe sustentar a la política, por ejemplo, políticas de seguridad más detalladas y procedimientos para sistemas de información específicos o reglas de seguridad que deben cumplir los usuarios.

La organización debe comunicar esta política a los usuarios de una manera relevante, accesible y entendible para el lector.

b) **Propiedad y análisis:** Debe programarse el proceso de revisión para realizar verificaciones periódicas de:

1. La efectividad de la política, la cual se demuestra mediante la naturaleza, número e impacto de los incidentes de seguridad registrados.

2. El costo e impacto de los controles sobre la eficiencia del negocio.

3. Los efectos tras realizar cambios de tecnología.

APÉNDICE B

SEGURIDAD DE LA ORGANIZACIÓN

a) **Foro para el manejo de la seguridad de la información:** el foro debe estar formado por un cuerpo administrativo existente, ya que tiene como objetivo encargarse de:

1. Revisar y aprobar la política de seguridad de la información y todas sus responsabilidades.

2. Supervisar los cambios significativos de los activos de información en caso de exponerse a amenazas mayores.

3. Revisar y supervisar incidentes de seguridad de la información.

4. Aprobar mejores iniciativas para incrementar la seguridad de la información.

Un administrador debe ser responsable de todas las actividades relacionadas con la seguridad.

b) **Coordinación del sistema de seguridad de la información:** este grupo:

1. Está de acuerdo con los roles específicos y las responsabilidades de seguridad de la información en toda la organización.

2. Está de acuerdo con las metodologías específicas y los procesos de seguridad de la información.

3. Está de acuerdo y sustenta las iniciativas de seguridad de la información de la organización.

4. Asegura que la seguridad es parte del proceso de planeamiento de la información.

5. Revisa los incidentes de seguridad de la información.

6. Promueve el manifiesto del negocio para la seguridad de la información en la organización.

7. Determina qué es adecuado y coordina la implementación de controles específicos de seguridad de la información en sistemas o servicios nuevos.

c) **Responsabilidades de la seguridad de la información:** los dueños de los recursos de información deben delegar sus responsabilidades de seguridad a los administradores individuales o proveedores de servicio, sin embargo, el dueño es responsable de la seguridad de los activos y debe ser capaz para determinar que cualquier responsabilidad delegada ha sido relevada correctamente. Es esencial que se establezca las áreas en las cuales cada administrador es responsable, para esto:

1. Deben identificarse y claramente definirse activos y procesos de seguridad asociados con cada sistema individual.

2. El administrador responsable de cada activo o proceso de seguridad debe estar de acuerdo y es indispensable documentar de manera detallada esta responsabilidad.

3. Deben definirse y documentarse de manera clara los niveles de autorización.

d) **Procesos de autorización:** debe establecerse un proceso de administración para la autorización de nuevos medios de procesamiento de información. Es necesario considerar los siguientes controles:

1. Los nuevos medios deben tener una aprobación apropiada de la administración del usuario, autorizando sus propósitos y usos. Debe obtenerse la aprobación con base en la responsabilidad del administrador para mantener el ambiente de seguridad del sistema local de información y asegurar que las políticas y los requerimientos relevantes de seguridad se mantengan.

2. Cuando sea necesario, tanto el hardware como el software se debe verificar para asegurar que son compatibles con otros componentes del sistema.

3. Debe autorizarse el uso de medios de procesamiento de información personal para el procesamiento de la información del negocio y cualquier control necesario.

4. Debe determinarse y autorizarse el uso de medios de procesamiento de información personal en el lugar de trabajo ya que puede causar nuevas vulnerabilidades.

Los incisos e) Especialista en seguridad de la información, f) Cooperación administrativa y g) Análisis independiente, no cuentan con información adicional.

h) Acceso de la tercera entidad:

Identificación de riesgos por el acceso de una tercera entidad

El tipo de acceso dado a terceros es de importancia especial, por ejemplo, los riesgos del acceso a través de una conexión de red son diferentes a los riesgos que resultan del acceso físico. Los tipos de acceso que se consideran son:

1. Acceso físico: a las oficinas, salas de computadoras, gabinetes.

2. Acceso lógico: a las bases de datos de una organización, sistemas de información.

A las terceras entidades se les puede conceder el acceso debido a ciertas razones, por ejemplo, hay terceras entidades que proporcionan servicios a una organización y no se localizan internamente, pero se les puede conceder el acceso físico y lógico a:

1. El personal de soporte de software y de hardware que necesita el acceso a la funcionalidad de una aplicación al nivel de sistema o de nivel bajo.

2. Los compañeros comerciales o empresas de riesgo compartido, que pueden intercambiar información, acceso a sistemas de información o compartir bases de datos.

La información se puede poner en riesgo por el acceso de terceros con una administración inadecuada de la seguridad. Cuando existe la necesidad del negocio de conectarse con un tercer sitio, es indispensable realizar una evaluación de riesgo para identificar cualquier requerimiento de controles específicos. También debe considerarse el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera entidad y las implicaciones de este acceso a la seguridad de la información de la organización. Las terceras entidades que son internas por un período de tiempo según lo definido en su contrato, pueden dar

lugar a debilidades en la seguridad. Ejemplos de terceros internos incluyen:

1. Mantenimiento del hardware y del software y el personal de ayuda.

2. Limpieza, abastecimiento, guardias de seguridad y otros servicios externos de apoyo.

3. Estudiantes, prácticas profesionales y otros trabajos ocasionales a corto plazo.

4. Consultores.

Es esencial conocer qué controles son necesarios para administrar el acceso de terceros a los medios de procesamiento de información de la organización. Generalmente, todos los requerimientos de seguridad resultantes del acceso de la tercera entidad o los controles internos, se reflejan en el contrato de la tercera entidad, por ejemplo, si hay una necesidad especial de confidencialidad de la información, se utilizan acuerdos de no divulgación. El acceso a la información y a los medios de procesamiento de información a través de una tercera entidad, no debe proporcionarse hasta que se hayan puesto en ejecución los controles apropiados y se firme un contrato, en éste se definen los términos para realizar la conexión o el acceso. Las acciones que implica el acceso de terceros a los medios de procesamiento de información de la organización se basan en un contrato formal que contiene o se refiere a todos los requerimientos de seguridad, esto para garantizar el cumplimiento con base en las políticas y los estándares de seguridad de la organización. El contrato debe asegurar que no haya un malentendido entre la organización y los terceros.

Los términos listados a continuación se consideran para su inclusión en el contrato (*Lista B.1*):

1. La política general de seguridad de la información.

2. Protección del activo, incluyendo:

   - Procedimientos para proteger los activos de la organización, incluyendo la información y el software.

- Procedimientos para determinar si ha ocurrido cualquier compromiso de los activos, por ejemplo, pérdida o modificación de datos.

- Controles para asegurar el regreso o la destrucción de la información y activos al final de, o en un punto convenido en tiempo durante el contrato.

- Integridad y disponibilidad.

- Restricciones en el copiado y divulgación de la información.

3. Una descripción de cada servicio que se hará disponible.

4. El nivel del servicio y los niveles inaceptables del servicio.

5. Disposición para la transferencia del personal cuando sea apropiado.

6. Las responsabilidades respectivas de las partes del acuerdo.

7. Las responsabilidades con respecto a los asuntos legales, por ejemplo, legislación de la protección de los datos, considerando especialmente diversos sistemas legislativos nacionales si el contrato implica la cooperación con organizaciones en otros países.

8. Los derechos de propiedad intelectual, asignación de los derechos de copia y protección de cualquier trabajo de colaboración.

9. Los acuerdos de control de acceso, cubriendo:

   - Métodos de acceso permitidos, el control y el uso de identificadores únicos tales como ID de usuario y contraseñas.

   - Un proceso de autorización para el acceso y los privilegios del usuario.

   - Un requerimiento para mantener una lista de los individuos autorizados para utilizar los servicios que están disponibles y cuáles son sus derechos y privilegios con respecto a tal uso.

10. El derecho de supervisar y revocar la actividad del usuario.

11. El derecho de revisar responsabilidades contractuales[31] o de hacer esas revisiones a través de una tercera entidad.

12. El establecimiento de un proceso para la resolución del problema; deben considerarse las acciones para la contingencia cuando sea apropiado.

13. Responsabilidades con respecto al hardware e instalación y mantenimiento del software.

14. Una estructura de divulgación clara y formatos de divulgación convenidos.

15. Un claro y específico proceso de administración del cambio.

16. Controles y mecanismos físicos de protección que aseguren que esos controles se siguen.

17. Capacitación del usuario y del administrador en métodos, procedimientos y seguridad.

18. Controles para asegurar la protección contra el software malicioso.

19. Arreglos para divulgar, notificar e investigar los incidentes de seguridad y las brechas en seguridad.

20. Implicación de terceros con los subcontratistas.

i) Outsourcing (organización externa):

Requerimientos de seguridad en contratos de outsourcing

Los requerimientos de seguridad de una organización que realiza el outsourcing de la administración y el control de todos o algunos de sus sistemas de información, redes y/o ambientes de escritorio se deben tratar

[31] Estipulados por contrato

en un contrato convenido entre las entidades. Por ejemplo, el contrato debe tratar:

1. Cómo satisfacer los requerimientos legales, por ejemplo, legislación de la protección de los datos.

2. Qué arreglos internos aseguran que todas las partes implicadas en el outsourcing, incluyendo subcontratistas, se enteren de sus responsabilidades de seguridad.

3. Cómo mantener y probar la integridad y la confidencialidad de los activos de negocio de la organización.

4. Qué controles físicos y lógicos utilizar para restringir y limitar el acceso sólo a los usuarios autorizados a la información sensible de negocio de la organización.

5. Cómo mantener la disponibilidad de los servicios cuando ocurre un desastre.

6. Qué niveles de seguridad física proveer para el equipo externo.

7. El derecho de auditar.

Los términos dados en la *lista B.1* también se deben considerar como parte de este contrato. El contrato permite que los requerimientos y los procedimientos de seguridad se amplíen en un plan de administración de seguridad que entre las dos entidades convienen. Aunque los contratos del outsourcing pueden plantear algunas preguntas complejas de seguridad, los controles incluidos en este código de práctica podrían servir como punto de partida para convenir la estructura y el contenido del plan de administración de seguridad.

APÉNDICE C

CLASIFICACIÓN Y CONTROL DE ACTIVOS

a) **Responsabilidad e inventario:** ejemplos de activos asociados a los sistemas de información son:

1. Activos de información: los archivos de datos y de las bases de datos, la documentación del sistema, los manuales de usuario, material de capacitación, procedimientos operacionales o de ayuda, planes de continuidad, información archivada.

2. Activos del software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.

3. Activos físicos: material informático (procesadores, monitores, computadoras portátiles, módems), equipo de comunicaciones (encaminadores, máquinas de fax, contestadoras automáticas), medios magnéticos (cintas y discos), otro equipo técnico (fuentes de alimentación, unidades de aire acondicionado), muebles.

4. Servicios: servicios de cómputo y de comunicaciones, utilidades generales, por ejemplo, calefacción, iluminación, energía, aire acondicionado.

b) **Clasificación:** la información y la salida de los sistemas que manejan datos clasificados se deben etiquetar con base en el valor y sensibilidad que tienen para la organización, puede ser apropiado etiquetarla en términos de qué tan crítica es para la organización o con base en su integridad y disponibilidad. La información deja a menudo de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se hace pública. Estos aspectos se toman en cuenta, pues la reclasificación puede conducir a un costo de negocio adicional e innecesario. Las pautas de la clasificación deben anticipar y permitir el hecho de que la clasificación de cualquier artículo de información no es necesariamente fija todo el tiempo, y puede cambiar con base en una cierta política predeterminada, para ello, se toma en cuenta el número de categorías de clasificación y las ventajas que se obtienen según el uso. Los esquemas complejos pueden llegar a ser excesivamente incómodos y poco rentables para utilizarlos o nada prácticos para probarlos.

Debe tenerse cuidado al interpretar etiquetas de clasificación en documentos de otras organizaciones que puedan tener diversas definiciones en etiquetas iguales o semejantes. La responsabilidad debe

recaer en el autor o el dueño nombrado de la información al definir la clasificación de un artículo de información - un registro de datos, un documento, un archivo de datos o un disco - y su revisión periódica.

c) **Etiquetado y manejo:** la manipulación de estos procedimientos se define para cada clasificación y para cubrir los siguientes tipos de procesamiento de la información:

1. Copiado.

2. Almacenamiento.

3. Transmisión por correo, fax y correo electrónico.

4. Transmisión mediante el uso de la palabra, incluyendo el teléfono celular, correo de voz, contestadoras automáticas.

5. Destrucción.

La salida de los sistemas que contienen información clasificada como sensible o crítica debe contar con una etiqueta apropiada de clasificación (en la salida), el etiquetado refleja la clasificación según las reglas establecidas por la organización. Los artículos que se consideran incluyen los informes impresos, exhibiciones de la pantalla, medios registrados (cintas, discos, CD, cassettes), mensajes electrónicos y transferencias de archivos. Las etiquetas físicas son generalmente las formas más apropiadas de etiquetado, sin embargo, algunos activos de información, tales como documentos en forma electrónica, no se pueden etiquetar físicamente y para hacerlo se necesitan medios electrónicos.

APÉNDICE D

SEGURIDAD DEL PERSONAL

a) Proyección personal:

Investigación del personal y política

Las pruebas de verificación del personal permanente se realizan al momento de la solicitud del empleo. Esto debe incluir los controles siguientes:

1. Disponibilidad de referencias satisfactorias de carácter, una de negocios y una personal.

2. Una prueba (para complementar y tener exactitud) del curriculum vitae del solicitante.

3. Confirmación de calificaciones académicas y profesionales.

4. Prueba independiente de la identidad (pasaporte o documento similar).

Si un trabajo, en la cita inicial o en la promoción, implica a una persona que tiene acceso a los medios de procesamiento de la información y si éstos manejan información sensible - información financiera o información altamente confidencial - la organización también debe realizar una prueba de su crédito; cuando el personal maneja posiciones de autoridad considerable esta prueba debe repetirse periódicamente, un proceso de investigación similar debe realizarse a los contratistas y al personal temporal. Si una agencia proporciona al personal, en el contrato con ésta, es indispensable especificar claramente las responsabilidades de la agencia para investigar y los procedimientos de a seguir en caso de que la investigación no se haya terminado o si los resultados dan lugar a dudas o preocupaciones. La administración debe evaluar la supervisión que se requiere para el nuevo e inexperto personal que cuenta con autorización para tener acceso a los sistemas sensibles. Es necesario que el trabajo de todo el personal esté sujeto a procedimientos periódicos de revisión y de aprobación por un miembro mayor del personal. Los encargados deben estar enterados de que las circunstancias particulares de su personal pueden afectar su trabajo, los problemas personales o financieros, los cambios en el comportamiento o forma de vida, las ausencias reiterativas y la evidencia de tensión o depresión pueden conducir al fraude, error, hurto o a otras implicaciones de seguridad. Es vital manejar esta información

con base en la legislación apropiada y existente en la jurisdicción correspondiente.

Los incisos b) Responsabilidades de seguridad, c) Términos y condiciones de empleo, d) Capacitación, no cuentan con información adicional.

e) **Recurso:** es trascendental que la organización establezca un proceso disciplinario formal para tratar con los empleados que cometen brechas en la seguridad. Para tratar los incidentes correctamente es necesario recoger evidencia inmediatamente después de la ocurrencia. Un procedimiento de divulgación formal se debe establecer junto con un procedimiento de respuesta, precisando la acción que se ejercerá como respuesta al reporte del incidente. Todos los empleados y contratistas deben enterarse del procedimiento para divulgar incidentes de seguridad y hacerlo lo más rápidamente posible, los procesos convenientes de regeneración se deben ejecutar para asegurar que aquéllos que reportan incidentes están notificados de los resultados después de que el incidente se haya tratado. Estos incidentes se pueden utilizar en la capacitación del usuario como ejemplos de lo que podría suceder, cómo responder a tales incidentes, y cómo evitarlos en el futuro.

Es necesario que los usuarios de servicios de información anoten y reporten cualquier debilidad que observen en la seguridad, amenazas a sistemas o servicios y las reporten al administrador o directamente al proveedor del servicio lo más rápidamente posible. Los usuarios deben estar informados de que no pueden, bajo ninguna circunstancia, probar debilidades sospechosas, esto es para su propia protección, ya que las debilidades de prueba se pueden interpretar como un mal uso potencial sistema. Para divulgar los malos funcionamientos del software se establecen procedimientos. Se consideran las acciones siguientes:

1. Indicar los síntomas del problema y de cualquier mensaje que aparecen en la pantalla.

2. La computadora debe aislarse, si es posible, terminar su uso, alertar al contacto apropiado inmediatamente. Si el equipo se examina, se debe desconectar de cualquier red antes de ser reconectado. Los diskettes no deben transferirse a otras computadoras.

3. El problema se debe reportar inmediatamente al encargado de la seguridad de la información.

Los usuarios no pueden quitar el software sospechoso a menos que estén autorizados para hacerlo y sólo el personal entrenado apropiadamente y experimentado debe realizar la recuperación del sistema.

Es vital que existan mecanismos en el lugar para permitir que los tipos, los volúmenes y los costos de los incidentes y de los malos funcionamientos se cuantifiquen y se supervisen, se utiliza esta información para identificar incidentes de alto impacto o malos funcionamientos recurrentes. Esto puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, el daño y el costo de ocurrencias futuras, o considerarse en el proceso de revisión de la política de seguridad.

Debe crearse un proceso disciplinario formal para los empleados que violen políticas y procedimientos de seguridad de la organización, tal proceso puede actuar como un impedimento para aquéllos que desatienden los procedimientos de seguridad, además, debe asegurar el tratamiento correcto y justo para los empleados que se sospecha pueden cometer brechas serias o persistentes en la seguridad.

APÉNDICE E

SEGURIDAD FÍSICA Y AMBIENTAL

a) Perímetro físico de la seguridad:

Las pautas y los controles siguientes deben considerarse e implementarse de manera apropiada:

1. Definir el perímetro de seguridad claramente.

2. El perímetro de un edificio o de un sitio que contiene medios de procesamiento de la información debe ser físicamente seguro (es decir, no debe haber boquetes en el perímetro o las áreas donde un robo podría ocurrir fácilmente). Las paredes externas del sitio deben construirse de manera sólida y todas las puertas externas se deben proteger convenientemente contra el acceso no autorizado - mecanismo de control, barras, alarmas, cerraduras.

3. Un área de recepción u otros medios para controlar el acceso físico al lugar o al edificio. El acceso a los lugares y a los edificios se debe restringir solamente al personal autorizado.

4. Las barreras físicas deben, en caso de ser necesario, extenderse desde el piso hasta el techo para prevenir la entrada no autorizada y la contaminación del medio ambiente – incendio, inundación.

5. Todas las puertas contra fuego en un perímetro de seguridad deben contar con alarma y cerrarse de golpe.

b) Control de acceso: se deben considerar los controles siguientes:

1. Los visitantes de áreas seguras se deben supervisar y es conveniente registrar su fecha y hora de entrada y salida. Sólo se les puede conceder el acceso para propósitos específicos, autorizados y se deben publicar las instrucciones sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

2. Debe controlarse el acceso a la información sensible y a los medios de procesamiento de la información y restringirse a personas autorizadas. Los controles de autenticación se utilizan para autorizar y para validar el acceso.

3. Todo el personal debe usar una identificación visible y cuestionar a cualquier persona que no la utilice.

4. Los derechos de acceso a áreas seguras deben revisarse y actualizarse regularmente.

Áreas seguras

Un área segura puede ser una oficina cerrada o varios cuartos dentro de un perímetro físico de seguridad, que puede estar cerrado y puede contener gabinetes o cajas fuertes. La selección y el diseño de un área segura toma en cuenta la posibilidad de daño por el fuego, inundación, explosión y otras formas de desastre natural o artificial. Es importante considerar la salud y las regulaciones y los estándares de seguridad, así como cualquier amenaza de seguridad que se presente en el entorno – como la salida de agua en otras áreas. Es vital considerar los controles siguientes:

1. Las instalaciones principales se deben localizar en un determinado lugar para evitar el acceso del público.

2. Los edificios deben ser discretos y dar la indicación mínima de su propósito, sin muestras obvias, fuera o dentro del edificio que identifiquen la presencia de las actividades de procesamiento de la información.

3. Las funciones de ayuda y el equipo - máquinas de fax, fotocopiadoras - se deben localizar apropiadamente dentro del área segura para evitar las demandas de acceso, que podría comprometer la información.

4. Las puertas y las ventanas deben estar cerradas cuando la protección externa se considera sólo para ventanas al nivel del suelo.

5. Los sistemas de detección de intrusos deben estar colocados en el lugar adecuado para cubrir todas las puertas externas y ventanas accesibles. Las áreas desocupadas deben tener siempre alarma y proporcionar algunas para otras áreas, por ejemplo, para la sala de computadoras o cuartos de comunicaciones.

6. Los medios de procesamiento de información manejados por la organización, se deben separar físicamente de aquéllos manejados por terceros.

7. Los directorios y las agendas de teléfono internos que identifican la ubicación de los medios de procesamiento de información, no deben ser fácilmente accesibles por el público.

8. Los materiales peligrosos o combustibles deben almacenarse con seguridad a una distancia adecuada de un área segura.

9. El equipo de resguardo y los medios de respaldo se deben localizar a una distancia adecuada para evitar daños si ocurre un desastre en el sitio principal.

Algunos controles adicionales y pautas se pueden requerir para aumentar la seguridad de un área segura, esto incluye los controles para el personal o terceros que trabajan en esta área segura, así como las actividades de los terceros que se realizan allí. Los controles siguientes deben tomarse en cuenta:

1. El personal debe estar enterado de la existencia de un área segura o de las actividades que en ella se realizan.

2. Debe evitarse el trabajo no supervisado en áreas seguras por razones de seguridad y para prevenir las oportunidades de actividades maliciosas.

3. Las áreas seguras vacantes deben estar físicamente cerradas y verificarse periódicamente.

4. Al personal externo de servicios de ayuda se le debe conceder acceso restringido a las áreas seguras o a los medios de procesamiento de la información solamente cuando se requiera. Este acceso debe ser autorizado y supervisado. Barreras adicionales y perímetros para controlar el acceso físico son necesarios entre áreas con diversos requerimientos de seguridad dentro del perímetro de seguridad.

5. El equipo fotográfico, de video, de audio u otro equipo de grabación no debe permitirse, a menos que esté autorizado.

Las áreas de entrega y carga deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. Los requerimientos de seguridad para tales áreas se determinan mediante una evaluación de riesgo. Se consideran los controles siguientes:

1. El acceso a un área desde el exterior del edificio se debe restringir sólo al personal identificado y autorizado.

2. El área debe diseñarse para poder descargar los suministros sin que el personal de entrega tenga acceso a otras partes del edificio.

3. Las puertas externas del área deben asegurarse cuando la puerta interna se abra.

4. El material entrante se debe examinar para evitar peligros potenciales antes de que se mueva desde el área de manejo hasta el lugar de uso.

5. El material entrante debe colocarse, si es apropiado, en la entrada del lugar.

c) Equipo:

Seguridad del equipo

El equipo se protege para reducir los riesgos de amenazas, los peligros ambientales y las oportunidades de acceso no autorizado. Los controles siguientes deben considerarse:

1. Para reducir al mínimo el acceso, el equipo innecesario debe ubicarse en áreas de trabajo.

2. El procesamiento de información y las instalaciones de almacenamiento que manejan datos sensibles se deben ubicar en el área para reducir el riesgo de descuido durante su uso.

3. Los artículos que requieren protección especial se deben aislar para reducir el nivel general de protección requerido.

4. Los controles se deben adoptar para reducir al mínimo el riesgo de amenazas potenciales incluyendo:

   - Hurto.
   - Fuego.
   - Explosivos.
   - Humo.
   - Agua (o falla de la fuente).
   - Polvo.
   - Vibración.
   - Efectos de productos químicos.
   - Interferencia de la fuente eléctrica.
   - Radiación electromagnética.

5. Una organización debe considerar en su política el comer, beber y fumar en la proximidad a las instalaciones de procesamiento de la información.

6. Las condiciones ambientales se deben supervisar para cuáles podrían afectar a la operación de las instalaciones de procesamiento de la información.

7. Se debe considerar el uso de métodos especiales de protección, tales como membranas para el teclado, para el equipo en ambientes industriales.

8. Debe considerarse el impacto de un desastre que sucede en sitios cercanos - fuego en un edificio vecino, el agua que se escapa de la azotea o a nivel subterráneo o una explosión en la calle.

Es importante proteger el equipo contra apagones y otras anomalías eléctricas, para esto, es conveniente proveer una fuente eléctrica adecuada al equipo y a las especificaciones del fabricante. Las opciones para alcanzar la continuidad de las fuentes de alimentación incluyen:

1. Múltiples alimentaciones para evitar una falla en la fuente de alimentación.

2. Fuente de alimentación continua (UPS).

3. Generador de respaldos.

Se recomienda una fuente de alimentación continua para el equipo de apoyo de las operaciones críticas del negocio - el equipo de la UPS se debe verificar regularmente para asegurar que tiene la capacidad adecuada y probada de acuerdo con las recomendaciones del fabricante -, es indispensable que los planes de contingencia cubran las acciones que se realizarán cuando no exista una fuente de alimentación continua.

Si el proceso debe continuar en caso de un apagón prolongado, es importante considerar un generador de respaldo, si están instalados, hay que probarlos regularmente de acuerdo con las instrucciones del fabricante. También debe disponerse de una fuente adecuada de combustible para asegurar que el generador funcione por un período prolongado. Otro punto a considerar son los interruptores de emergencia, los cuales se deben situar cerca de las salidas de emergencia en los cuartos del equipo para facilitar una baja de energía rápida en caso de una emergencia. Cuando exista una falla de en la alimentación principal de luz, es conveniente contar con luz de emergencia, ésta se debe proporcionar a todos los edificios junto con los filtros de protección de luz que se proveen a todas las líneas de comunicaciones externas. La energía y el cableado de telecomunicaciones que transportan datos o soportan servicios de información deben protegerse contra la intercepción o el daño. Para esto se consideran los controles siguientes:

1. Las líneas de energía y de telecomunicaciones en las instalaciones del procesamiento de información deben ser subterráneas, en lo posible, o según la protección alternativa adecuada.

2. El cableado de la red se debe proteger contra la intercepción o el daño no autorizado, por ejemplo, evitando las rutas a través de áreas públicas.

3. Los cables de energía se deben separar de los cables de comunicaciones para evitar la interferencia.

4. Para los sistemas sensibles o críticos se considera:

   - Instalación del conducto armado y de cuartos cerrados o cajas en los puntos de inspección y de terminación.
   - Uso de rutas o medios alternativos de transmisión.
   - Uso de cableado de fibra óptica.
   - Inspección de los dispositivos no autorizados que se unen a los cables.

Es trascendental mantener correctamente el equipo para asegurar su disponibilidad e integridad continuas. Deben tomarse en cuenta los controles siguientes:

1. El equipo se debe mantener de acuerdo con los intervalos y las especificaciones recomendados por el proveedor del servicio.

2. Solamente el personal autorizado de mantenimiento debe realizar reparaciones y mantener el equipo.

3. En los registros se deben anotar todas las fallas y todo el mantenimiento preventivo y correctivo.

4. Deben ser tomados en cuenta los controles apropiados al enviar el equipo fuera de las instalaciones para su mantenimiento y se deben cumplir todos los requerimientos impuestos por pólizas de seguro.

d) **Transferencia de archivos:** la seguridad que se proporciona debe ser equivalente a la del equipo que se encuentra interno se usa para el mismo propósito, considerando los riesgos del trabajo fuera de las instalaciones de la organización. El equipo de procesamiento de la información incluye las

computadoras personales, organizadores, teléfonos celulares, papel u otra forma que se utiliza para realizar el trabajo en el hogar o que se transporta lejos de la ubicación normal de trabajo. Las pautas siguientes se consideran:

1. El equipo y los medios que se extraen de las instalaciones no se deben desatender en lugares públicos. Las computadoras portátiles deben ser llevadas como equipaje de mano y disfrazarse al viajar.

2. Las instrucciones de los fabricantes para proteger el equipo se deben considerar siempre - protección contra la exposición a campos electromagnéticos fuertes.

3. Los controles para el hogar-trabajo se deben determinar mediante una evaluación de riesgo y aplicarse - gabinetes cerrados, política de limpieza de escritorio y los controles de acceso para las computadoras.

4. Debe existir un seguro adecuado en el lugar para proteger el equipo que se encuentre fuera del sitio.

Los riesgos de seguridad como el daño, hurto y el escuchar detrás de las puertas, pueden variar considerablemente entre lugares y pueden considerarse para determinar los controles más apropiados.

La información se puede comprometer con la disposición o la reutilización descuidada del equipo. Los dispositivos de almacenamiento que contienen información sensible se deben destruir o sobreescribir con seguridad. Es importante que todos los accesorios del equipo que contienen medios de almacenamiento como discos duros fijos, se verifiquen para asegurar que los datos sensibles y el software se hayan quitado o se hayan sobrescrito antes de su disposición. Los dispositivos de almacenamiento dañados que contienen datos sensibles pueden requerir una evaluación de riesgo para determinar si se destruyen, se reparan o se desechan.

e) **General:** las organizaciones deben considerar la aplicación de una política de limpieza de escritorio para los papeles y los medios de almacenamiento removibles y una política de limpieza de pantalla para las instalaciones de procesamiento de información con el objetivo de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante y fuera de

las horas normales de trabajo. Esta política considera las clasificaciones de seguridad de la información, los riesgos correspondientes y los aspectos culturales de la organización. La información que se deja sobre los escritorios puede dañase o destruirse en un desastre tal como un incendio, una inundación o una explosión. Es conveniente considerar los controles siguientes:

1. Cuando sea apropiado, los papeles y la computadora se deben almacenar en gabinetes cerrados y/o en otros muebles de seguridad cuando no estén en uso, especialmente fuera de las horas de trabajo.

2. La información sensible o crítica del negocio se debe guardar (idealmente en un lugar resistente al fuego o un gabinete) cuando no se requiera, especialmente cuando se desocupa la oficina.

3. Las computadoras personales, las terminales y las impresoras no se deben dejar conectadas cuando se desatiendan y se deben proteger cuando no estén en uso mediante teclas como candados, contraseñas u otros controles.

4. Deben protegerse los puntos entrantes y salientes del correo, el fax desatendido y las máquinas de Telex.

5. Las fotocopiadoras deben bloquearse o protegerse contra el uso no autorizado en horas fuera de trabajo.

6. La información sensible o clasificada, cuando se imprime, debe retirarse inmediatamente de las impresoras.

El equipo, la información o el software no deben salir del lugar sin autorización, si la salida es necesaria, el equipo debe registrar la fecha y hora de su salida y su devolución. Es necesario realizar verificaciones al azar para detectar el retiro no autorizado de los equipos, los individuos deben enterarse que se realizarán estas verificaciones.

APÉNDICE F

GESTIÓN DE COMUNICACIONES Y OPERACIONES

a) **Procedimientos operacionales:** es conveniente que los procedimientos especifiquen las instrucciones detalladas para la implementación de cada trabajo, incluyendo:

1. Procesamiento y manejo de la información.

2. Requerimientos de horarios, incluyendo interdependencias con otros sistemas, el comienzo más temprano del trabajo y los tiempos más tardes de la terminación del trabajo.

3. Instrucciones para manejar los errores u otras condiciones excepcionales, que pueden presentarse durante la ejecución del trabajo, incluyendo restricciones en el uso de las utilidades de sistema.

4. Contactos de ayuda en eventos operacionales inesperados o dificultades técnicas.

5. Instrucciones especiales de manejo de la salida, tales como el uso de equipo especial o la administración de la salida confidencial, incluyendo los procedimientos para la disposición segura de la salida de trabajos fallidos.

6. Reinicio del sistema y procedimientos de recuperación para su uso cuando existan fallas del sistema.

Se deben elaborar y documentar los procedimientos junto con las actividades cotidianas del sistema asociadas al procesamiento de la información y a las instalaciones de comunicación, tales como los procedimientos de encendido, apagado, respaldo, mantenimiento del equipo, sala de computadoras y la administración del manejo del correo y la seguridad.

b) **Control de cambios:** es conveniente que las responsabilidades y los procedimientos formales de la administración se encuentren en el lugar para asegurar el control satisfactorio de todos los cambios al equipo, al software o a los procedimientos. Los programas operacionales se encuentran sujetos a un estricto control de cambio, cuando se realiza un cambio en los programas, debe realizarse un registro que contenga toda la información relevante. Los cambios al ambiente operacional pueden afectar las aplicaciones, por eso, deben integrarse procedimientos

practicables, operacionales y de aplicación de control de cambios. En detalle, los controles siguientes se consideran:

1. Identificación y registro de cambios significativos.

2. Evaluación del impacto potencial de tales cambios.

3. Procedimiento formal de aprobación para los cambios propuestos.

4. Comunicación de los detalles del cambio a todas las personas relevantes.

5. Procedimientos que identifican las responsabilidades de aborto y recuperación de los cambios no exitosos.

c) **Manejo de incidentes:** los controles siguientes deben considerarse:

1. Los procedimientos se deben establecer para cubrir todos los tipos potenciales de incidente de seguridad, incluyendo:

   - Fallas del sistema de información y pérdida de servicio.

   - Denegación del servicio.

   - Errores como resultado de datos de negocio incompletos o inexactos.

   - Brechas en la confidencialidad.

2. Además del plan de contingencia normal (diseñado para recuperar sistemas o servicios lo más rápidamente posible) los procedimientos deben también cubrir:

   - Análisis e identificación de la causa del incidente.

   - Planeación e implementación de remedios para prevenir la recurrencia, en caso de ser necesario.

   - Colección de indicios de auditoría y evidencia similar.

- Comunicación con los afectados o implicados con la recuperación del incidente.

- Reportar la acción a la autoridad correspondiente.

3. Los indicios de auditoría y la evidencia similar deben recolectarse apropiadamente para:

   - Un análisis interno del problema.

   - Uso como evidencia en lo referente a una brecha potencial en el contrato, una brecha en el requerimiento regulador o si ocurren procedimientos civiles o criminales – mal uso de la computadora o en la legislación de la protección de datos.

   - Negociación para la remuneración de los proveedores del software y del servicio.

4. Acciones para recuperarse de las brechas en la seguridad y fallas del sistema deben estar cuidadosamente controladas. Estos procedimientos deben asegurar que:

   - Solamente al personal claramente identificado y autorizado se le permite el acceso a los sistemas y a los datos.

   - Todas las medidas de emergencia tomadas se documenten detalladamente.

   - Las medidas de emergencia se divulguen a la administración y se revisen de una manera ordenada.

La integridad de los sistemas y de los controles del negocio se confirme con un retraso mínimo.

d) Separación de deberes: las organizaciones pequeñas pueden encontrar este método de control difícil de implementar, pero el principio se debe aplicar hasta donde sea posible y practicable. Siempre que sea difícil separar, otros controles deben considerarse tales como la supervisión de actividades, pistas de auditoría y la supervisión de la administración. Es

importante que la auditoría de seguridad siga siendo independiente. Debe tenerse cuidado de que alguna persona pueda perpetrar fraude en áreas de poca responsabilidad sin ser detectado. Los controles siguientes deben considerarse:

1. Es importante separar las actividades que requieren la colusión[32] para defraudar, por ejemplo, levantando una orden de compra y verificando que se han recibido las mercancías.

2. Si hay peligro de colusión, entonces los controles necesitan ser ideados de tal modo que dos o más personas necesiten estar implicados, esto reduce la posibilidad de conspiración.

Separación del desarrollo y de las instalaciones operacionales

Al separar el desarrollo, las pruebas y las instalaciones operacionales es importante alcanzar la segregación de los papeles implicados. Las reglas para la transferencia del software de desarrollo al estado operacional deben definirse y documentarse. El desarrollo y las actividades de prueba pueden causar problemas serios - modificación no deseada de archivos o del ambiente del sistema o fallas del sistema -, por eso, es importante considerar el nivel de separación necesario entre ambientes operacionales de prueba y desarrollo, para prevenir problemas operacionales. Una separación similar debe implementarse entre funciones de desarrollo y prueba, en este caso, existe la necesidad de mantener un ambiente conocido y estable en el cual se realicen pruebas significativas y se prevenga el acceso innecesario del desarrollador. En algunos lugares el personal de desarrollo y de prueba tiene acceso al sistema operacional y a su información y puede introducir código no autorizado y no probado o alterar datos operacionales, en algunos sistemas esta capacidad puede ser mal usada para cometer fraude, o introducir código no probado o malicioso - el código no probado o malicioso puede causar problemas operacionales serios. Los desarrolladores y los probadores también plantean una amenaza a la confidencialidad de la información operacional ya que las actividades de desarrollo y prueba pueden causar cambios involuntarios al software y a la información si comparten el mismo ambiente de cómputo. Al separar el desarrollo, la prueba y las instalaciones operacionales se reduce el riesgo de cambios accidentales o

[32] Convenio o trato entre varios con intención de perjudicar a otro

de acceso no autorizado al software operacional y a los datos de negocio. Es trascendental considerar los controles siguientes:

1. El desarrollo y el software operacional, cuando es posible, se ejecutan en diversos procesadores de computadora, o en diversos dominios o directorios.

2. Las actividades de desarrollo y de prueba se deben separar lo más quw se pueda.

3. Los compiladores, los editores y otras utilidades del sistema no deben ser accesibles desde sistemas operacionales cuando esto no se requiera.

4. Diversos procedimientos de conexión se deben utilizar en sistemas operacionales y de prueba para reducir el riesgo de error. Los usuarios deben ser aconsejados para que utilicen diversas contraseñas en estos sistemas, y los menús deben exhibir mensajes apropiados de identificación.

5. El personal de desarrollo debe tener acceso solamente a las contraseñas operacionales cuando hay controles en el lugar que permiten la publicación de contraseñas para lograr el soporte de sistemas operacionales. Los controles deben asegurarse de que tales contraseñas se cambien después de su aplicación.

Administración de instalaciones externas

El uso de un contratista externo para manejar las instalaciones de procesamiento de la información puede introducir exposiciones potenciales de seguridad, tales como la posibilidad de compromiso, de daño, o de pérdida de datos en el sitio del contratista. Estos riesgos se deben identificar por adelantado y los controles apropiados deben convenirse con el contratista e incorporarse en el contrato. Los puntos particulares que deben ser tratados incluyen:

1. Identificación de aplicaciones sensibles o críticas que deben conservarse mejor internamente.

2. Obtención de la aprobación de los dueños de la aplicación del negocio.

3. Implicaciones para los planes de continuidad del negocio.

4. Estándares de seguridad que se especifican, y el proceso para medir el cumplimiento.

5. Asignación de responsabilidades específicas y procedimientos para supervisar con eficacia todas las actividades relevantes de seguridad.

6. Responsabilidades y procedimientos para divulgar y manejar incidentes de seguridad.

El inciso e) Planificación de la capacidad, no contiene información adicional.

f) Aceptación del sistema: los encargados deben asegurarse de que los requerimientos y los criterios para la aceptación de nuevos sistemas, estén definidos claramente, convenidos, documentados y probados. Hay que considerar los controles siguientes:

1. Ejecución y requerimientos de la capacidad de la computadora.

2. Procedimientos de recuperación de error, reinicio y planes de contingencia.

3. Preparación y prueba de procedimientos de operación rutinarios para definir estándares.

4. Conjunto de controles de seguridad convenidos en el lugar.

5. Procedimientos manuales eficaces.

6. Arreglos de la continuidad del negocio con base en los requerimientos de la sección *Plan de continuidad del negocio*.

7. Evidencia de que la instalación del nuevo sistema no afectará a los sistemas existentes, particularmente en los tiempos de procesamiento máximos, por ejemplo, a fin de mes.

8. Evidencia de que se considera el efecto que tiene el nuevo sistema en la seguridad total de la organización.

9. Capacitación en la operación o el uso de nuevos sistemas.

Es conveniente que los desarrolladores consulten, en todas las etapas del proceso de desarrollo, las funciones de operación y a los usuarios para asegurar la eficacia operacional del diseño propuesto del sistema, deben realizarse pruebas apropiadas para confirmar que todos los criterios de aceptación se satisfacen completamente.

g) **Código malicioso:** los controles de detección y de prevención que protegen contra software malicioso deben implementarse junto con procedimientos apropiados que alerten al usuario, ya que la protección contra éste se basa en alertas de seguridad, acceso apropiado del sistema y controles de administración del cambio, es indispensable considerar los controles siguientes:

1. Una política formal que se cumple con software autorizado y que prohíbe el uso del software no autorizado.

2. Una política formal para proteger contra los riesgos asociados a los archivos y el software que se obtienen vía redes externas, o por cualquier otro medio, indicando las medidas protectoras que deben tomarse.

3. Instalación y actualización regular de antivirus y software de reparación para explorar las computadoras y los medios como control preventivo o de manera rutinaria.

4. Conducir revisiones regulares del software y del contenido de los datos de los sistemas que soportan procesos críticos del negocio. La presencia de archivos desaprobados o no autorizados debe investigarse formalmente.

5. Verificar cualquier archivo en medios electrónicos de origen incierto o no autorizado, o archivos recibidos desde redes no confiables, para evitar virus.

6. Verificar cualquier anexo al correo electrónico y las transferencias para saber si existe software malicioso. Esta verificación se puede realizar en diversos lugares - en los servidores de correo electrónico, las computadoras de escritorio o al ingresar en la red de la organización.

7. Procedimientos y responsabilidades de administración para ocuparse de la protección de virus en sistemas, capacitación en su uso, reporte y recuperación de ataques de virus.

8. Planes apropiados de la continuidad del negocio para recuperarse de ataques de virus, incluyendo todos los respaldos necesarios de los datos y recuperación del software.

9. Procedimientos para verificar toda la información referente a software malicioso y asegurar que los boletines de advertencia sean exactos e informativos. Los encargados deben asegurar que las fuentes calificadas - diarios respetables, sitios de Internet confiables o proveedores de software antivirus -, se utilicen para distinguir entre bromas y virus verdaderos. Es trascendental que el personal se entere del problema que causan las bromas y qué debe hacer al recibir una de ellas.

Estos controles son especialmente importantes en los servidores de archivo de red que soportan una gran cantidad de sitios de trabajo.

h) Doméstico:

Respaldo de información

Se deben realizar regularmente copias de respaldo de la información esencial para el negocio y del software. Deben proporcionarse instalaciones o medios adecuados para estos respaldos para asegurar que toda la información y el software esenciales del negocio, se pueden recuperar después de un desastre o de una falla en los medios. Es esencial que se pruebe regularmente a los respaldos de los sistemas individuales para asegurar que éstos resuelven los requerimientos de los planes de continuidad del negocio. Los controles siguientes deben considerarse:

1. Un nivel mínimo de información de respaldo, junto con los registros exactos y completos de las copias de respaldo y los procedimientos documentados de la restauración, se debe almacenar en un lugar remoto, con una distancia suficiente para escapar a cualquier daño causado por un desastre en el sitio principal. Deben conservarse por lo menos tres generaciones o ciclos de respaldo de información de las aplicaciones importantes para el negocio.

2. La información de respaldo debe recibir un nivel de protección física y ambiental adecuado consistente con los estándares aplicados en el sitio principal. Los controles aplicados a los medios en el sitio principal deben ampliarse para cubrir el sitio de respaldo.

3. Los medios de respaldo se deben probar regularmente, siempre que sea posible, para asegurarse de que son confiables para su uso en una emergencia.

4. Los procedimientos de restauración se deben comprobar y probar regularmente para asegurarse de que son eficaces y de que pueden completarse dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

Debe determinarse el período de validez de la información esencial del negocio y cualquier requerimiento para que la copia del archivo se conserve permanentemente.

Registros del operador

El personal operacional debe mantener un registro de sus actividades. Los registros deben incluir:

1. Tiempos en los que el sistema inicia y termina.

2. Errores del sistema y la acción correctiva a tomar.

3. Confirmación del correcto manejo de los archivos de datos y de la salida de la computadora.

4. El nombre de la persona que realiza la entrada del registro.

Es importante que los registros del operador se sujeten a pruebas regulares e independientes contra los procedimientos de operación. Las fallas deben reportarse y posteriormente tomar una acción correctiva, deben registrarse todas las fallas reportadas por los usuarios con respecto a problemas con el procesamiento de la información o los sistemas de comunicaciones. Reglas claras deben existir para manejar las fallas reportadas, incluyendo:

1. Revisión de los registros de fallas para asegurar que éstas se han resuelto satisfactoriamente.

2. Revisión de medidas correctivas para asegurar que los controles no se han comprometido y que la acción tomada está autorizada.

i) **Administración de red:** algunos controles adicionales se requieren para proteger los datos sensibles que pasan por las redes públicas, alcanzar y mantener la seguridad en las redes de computadoras. Los administradores de la red deben implementar controles para mantener la seguridad de los datos en las redes y la protección de los servicios conectados contra el acceso no autorizado. En detalle, los controles siguientes se deben considerar:

1. La responsabilidad operacional de las redes se debe separar de las operaciones de la computadora cuando sea apropiado.

2. Deben establecerse las responsabilidades y los procedimientos para la administración del equipo remoto, incluyendo el equipo en las áreas del usuario.

3. Si es necesario, se deben establecer controles especiales para mantener la confidencialidad y la integridad de los datos que pasan por redes públicas y para proteger los sistemas conectados. Los controles especiales se pueden requerir para mantener la disponibilidad de los servicios de la red y de las computadoras conectadas.

4. Las actividades de administración se deben coordinar de cerca para optimizar el servicio al negocio y para asegurar que los controles se aplican constantemente a través de la infraestructura de procesamiento de la información.

j) **Manejo de medios:** es necesario establecer procedimientos de operación apropiados para proteger los documentos, los medios de cómputo (cintas, discos, cassettes), entrada-salida de los datos y la documentación del sistema contra daño, hurto y el acceso no autorizado. Deben existir procedimientos para la administración de medios removibles de la computadora, tales como cintas, discos, cassettes e informes impresos. En este caso, se consideran los controles siguientes:

1. Deben borrarse, si ya no se requieren más, los contenidos anteriores de cualquier medio reutilizable que se retirará de la organización.

2. Se requiere autorización para remover los medios de la organización y es necesario mantener un registro de tales retiros.

3. Todos los medios deben almacenarse en un ambiente seguro de acuerdo con las especificaciones del fabricante.

4. Todos los procedimientos y niveles de autorización deben documentarse claramente.

Los medios se deben poner en orden de manera segura cuando ya no sean requeridos, ya que la información sensible se puede filtrar a personas exteriores debido a una distribución descuidada de éstos, es indispensable establecer procedimientos formales para su distribución segura y reducir al mínimo este riesgo. Los controles siguientes deben tomarse en cuenta:

1. Los medios que contienen información sensible se deben almacenar y distribuir con seguridad - incineración o destrozo, vaciar los datos para su uso por otra aplicación dentro de la organización.

2. La lista siguiente identifica los artículos que pueden requerir una disposición segura:

   - Documentos en papel.
   - Voz u otras grabaciones.
   - Papel carbón.
   - Reportes de salida.
   - Cintas de impresora de un solo uso.
   - Discos magnéticos.
   - Cassettes o discos removibles.

- Medios de almacenamiento ópticos (todas las formas e incluyendo todos los medios de distribución de software del fabricante).
- Listados del programa.
- Datos de prueba.
- Documentación del sistema.

3. Puede ser más fácil arreglar todos los medios recogidos y distribuidos con seguridad, que separar los artículos sensibles.

4. Muchas organizaciones ofrecen los servicios de colección y distribución para papeles, equipo y medios. Debe seleccionarse un contratista con controles y experiencia adecuados.

5. La distribución de artículos sensibles debe registrarse cuando sea posible para mantener un documento con esta información.

Al acumular los medios para la distribución, es trascendental considerar el efecto de agregación, que puede causar que una cantidad grande de información sin clasificar llegue a ser más sensible que una cantidad pequeña de información clasificada.

Procedimientos para el manejo de información

Se deben establecer procedimientos para el manejo y el almacenamiento de información para proteger tal información contra el acceso no autorizado o el mal uso, es conveniente elaborar procedimientos para manejar la información consistente con su clasificación en documentos, sistemas de cómputo, redes, cómputo móvil, comunicaciones móviles, correo electrónico, correo de voz, comunicaciones de voz en general, multimedia, servicios/instalaciones postales, uso de máquinas de fax y cualquier otro artículo sensible - cheques en blanco, facturas. Deben considerarse los siguientes controles:

1. Manejo y etiquetado de todos los medios.

2. Restricciones de acceso para identificar al personal no autorizado.

3. Mantenimiento de un registro formal de los receptores autorizados de datos.

4. Aseguramiento de que los datos de entrada estén completos, que el proceso se termine correctamente y que la validación de la salida se aplique.

5. Protección de los datos que aguardan salida a un nivel consistente con su sensibilidad.

6. Almacenamiento de medios en un ambiente que concuerda con las especificaciones de los fabricantes.

7. Mantener la distribución de datos a un mínimo.

8. Claro etiquetado de todas las copias de los datos para su atención por parte de los receptores autorizados.

9. Revisión de las listas de distribución y de las listas de receptores autorizados en intervalos regulares.

La documentación del sistema puede contener información sensible - descripciones de los procesos de aplicación, procedimientos, estructuras de datos, procesos de autorización. Los controles siguientes deben considerase para proteger la documentación del sistema contra el acceso no autorizado:

1. La documentación del sistema se debe almacenar con seguridad.

2. La lista de acceso a la documentación del sistema se debe guardar y autorizar por el dueño de dicha actividad.

3. La documentación del sistema que se lleva a cabo en una red pública, o es provista vía una red pública, debe protegerse apropiadamente.

k) Intercambio de información:

Acuerdos de intercambio de información y de software

Deben establecerse acuerdos, algunos de los cuales pueden ser formales incluyendo acuerdos de fideicomiso de software, para lograr el intercambio

de información y de software (si es electrónico o manual) entre las organizaciones, el contenido de seguridad de tales acuerdos debe reflejar la sensibilidad de la información implicada del negocio. Los acuerdos en condiciones de seguridad deben considerar:

1. Responsabilidades de administración para controlar y notificar la transmisión, el envío y el recibo.

2. Procedimientos para notificar al remitente, la transmisión, el envío y el recibo.

3. Estándares técnicos mínimos para empaquetar y transmitir.

4. Estándares para la identificación del mensajero.

5. Responsabilidades y riesgos en la pérdida de datos.

6. Uso de un sistema de etiquetado adecuado para la información sensible o crítica, asegurándose de que el significado de las etiquetas se entiende inmediatamente y que la información se protege apropiadamente.

7. Información y software pertenecientes y las responsabilidades de la protección de los datos, derechos reservados del software y consideraciones similares.

8. Estándares técnicos para la grabación y lectura de información y software.

9. Controles especiales que se requieren para proteger artículos sensibles como claves criptográficas.

La información puede ser vulnerable al acceso no autorizado, al mal uso o a la corrupción durante el transporte físico, por ejemplo, al enviar medios vía el servicio postal o vía un mensajero. Los controles siguientes se deben aplicar para salvaguardar los medios de la computadora que son transportados de un sitio a otro:

1. Deben utilizarse transportes o mensajeros confiables. Una lista de mensajeros autorizados se debe acordar con la administración e

implementar un procedimiento para comprobar la identificación de los mensajeros.

2. El empaquetado debe ser suficiente para proteger el contenido contra cualquier daño físico que probablemente pueda presentarse durante el traslado y de acuerdo con las especificaciones del fabricante.

3. Deben adoptarse controles especiales, cuando sea necesario, para proteger la información sensible contra el acceso o la modificación no autorizado. Por ejemplo:

   - Uso de contenedores cerrados.
   - Entrega manual.
   - Empaquetado evidentemente forzado (que revela cualquier tentativa de acceso).
   - En casos excepcionales, partir el envío en más de una entrega y enviar por diversas rutas.
   - Uso de firmas digitales y cifrado de confidencialidad.

Seguridad del comercio electrónico

El comercio electrónico implica el intercambio electrónico de datos, correo electrónico y transacciones en línea a través de redes públicas tales como el Internet, sin embargo, es vulnerable a un gran número de amenazas de la red que pueden dar lugar a actividad fraudulenta, conflicto del contrato y divulgación o modificación de la información, por eso es importante aplicar controles para proteger el comercio electrónico contra tales amenazas. Las consideraciones de seguridad para el comercio electrónico deben incluir los controles siguientes:

1. Autenticación: ¿Qué nivel de confianza debe requerir el cliente y el comerciante en la contraparte para demandar la identidad?.

2. Autorización: ¿Quién está autorizado para fijar precios, la impresión o la firma clave de los documentos comerciales? ¿Cómo sabe esto el socio comercial?.

3. Contrato y proceso de ofrecimiento: ¿Cuáles son los requerimientos para la confidencialidad, integridad y prueba de envío y recibo de los documentos claves y el no repudio de los contratos?.

4. Información de precios: ¿Qué nivel de confianza se puede poner en la integridad de la lista de precios y la confidencialidad de los arreglos sensibles de descuento?.

5. Transacciones de pedido. ¿Cómo es la confidencialidad y la integridad del pedido, la forma de pago, los detalles de la entrega, y la confirmación de recibo proporcionados?.

6. Revisión: ¿Qué grado de revisión es el apropiado para comprobar la información del pago provista por el cliente?.

7. Establecimiento. ¿Cuál es la forma más apropiada de pago para evitar el fraude?.

8. Pedido. ¿Qué protección se requiere para mantener la confidencialidad y la integridad de la información del pedido y para evitar la pérdida o la duplicación de las transacciones?.

9. Responsabilidad. ¿Quién tiene la responsabilidad cuando existen transacciones fraudulentas?.

Muchas de las consideraciones antes dichas se pueden tratar mediante el uso de técnicas criptográficas, considerando su cumplimiento con los requerimientos legales. Los arreglos de comercio electrónico entre los socios comerciales deben apoyarse en un acuerdo documentado, en el cual confíen ambas partes y en donde se indique los términos de comercio, incluyendo detalles de autorización, sin embargo, pueden ser necesarios otros acuerdos con proveedores de servicio de información y de valor añadido. Los sistemas públicos de comercio deben publicar sus términos de negocio a los clientes, siempre debe considerarse un posible ataque al anfitrión que es utilizado para el comercio electrónico y las implicaciones de seguridad en cualquier interconexión de red requerida para su puesta en práctica.

Seguridad del correo electrónico

El correo electrónico se utiliza para las comunicaciones del negocio, sustituyendo formas tradicionales de comunicación tales como el teléfono y las cartas. El correo electrónico difiere de las formas tradicionales de comunicaciones de negocio en su velocidad, estructura del mensaje, grado de informalidad y vulnerabilidad a acciones no autorizadas, por lo tanto, debe considerarse la necesidad de emplear controles para reducir los riesgos de seguridad creados por el correo electrónico. Los riesgos de seguridad incluyen:

1. Vulnerabilidad de los mensajes al acceso o modificación no autorizado o denegación del servicio.

2. Vulnerabilidad al error - dirección incorrecta -, la confiabilidad y disponibilidad generales del servicio.

3. Impacto de un cambio de los medios de comunicación en procesos de negocio - el efecto de aumentar la velocidad del envío o el efecto de enviar mensajes formales de una persona a otra en lugar de una compañía a otra.

4. Consideraciones legales, tales como la necesidad potencial de la prueba del origen, del envío, de la entrega y de la aceptación.

5. Implicaciones de publicar externamente listas accesibles del personal.

6. Controlar el acceso del usuario remoto a las cuentas de correo electrónico.

Las organizaciones deben redactar una política clara con respecto al uso del correo electrónico, incluyendo:

1. Ataques contra correo electrónico, por ejemplo, virus, intercepción.

2. Protección de los archivos adjuntos al correo electrónico.

3. Reglas sobre cuándo no utilizar el correo electrónico.

4. Responsabilidad del empleado para no comprometer a la compañía enviando correo electrónico difamatorio, utilizando hostigamiento o realizando compras no autorizadas.

5. Uso de técnicas criptográficas para proteger la confidencialidad y la integridad de los mensajes electrónicos.

6. Retención de mensajes que, si están almacenados, se pueden descubrir en caso de un litigio.

7. Controles adicionales para revisar los mensajes que no pueden ser autenticados.

Seguridad de los sistemas de oficina electrónica

Las políticas y las pautas se deben preparar e implementar para controlar los riesgos del negocio y de seguridad asociados a los sistemas de oficina electrónica, éstos proporcionan oportunidades para una rápida difusión y para compartir la información del negocio usando una combinación de: documentos, computadoras, computadoras portátiles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz, en general, multimedia, servicios/instalaciones postales y máquinas de fax. La consideración que se da a las implicaciones de seguridad y del negocio al interconectar tales medios debe incluir:

1. Vulnerabilidades de la información en los sistemas de oficina como grabación de llamadas telefónicas o llamadas de conferencia, confidencialidad de la llamada, almacenamiento de faxes, correo abierto, distribución del correo.

2. Política y controles apropiados para manejar la información compartida, como el uso de anuncios electrónicos corporativos.

3. Categorías de exclusión de información sensible del negocio si el sistema no proporciona un nivel apropiado de protección.

4. Acceso restringido a la información diaria referente a individuos seleccionados como el personal que trabaja en proyectos sensibles.

5. La adaptabilidad del sistema para soportar aplicaciones de negocio, tales como órdenes de comunicación o autorizaciones.

6. Las categorías del personal, contratistas o socios de negocio autorizados para utilizar el sistema y los lugares desde los cuales se puede tener acceso a éste.

7. Instalaciones o medios restringidos a categorías específicas de usuario.

8. Identificación del estado de los usuarios - empleados de la organización o contratistas - en directorios para beneficio de otros usuarios.

9. Retención y respaldo de la información del sistema.

10. Requerimientos y arreglos de retroceso.

Se debe poner cuidado en proteger la integridad de la información electrónicamente publicada para prevenir la modificación no autorizada que podría dañar la reputación de la organización que la publica. La información sobre un sistema disponible - información sobre un servidor de Web accesible vía Internet - puede necesitar cumplir con las leyes, reglas y regulaciones de la jurisdicción en donde el sistema se encuentra o donde ocurre el comercio. Debe existir un proceso formal de autorización antes de que la información se haga disponible públicamente. Es indispensable que el software, los datos y otra información que requieren un alto nivel de integridad, y que se encuentran disponibles en un sistema público, se proteja mediante un mecanismo apropiado, por ejemplo, firmas digitales. Los sistemas de publicación electrónica, especialmente los que permiten la retroalimentación y la entrada directa de información, deben estar cuidadosamente controlados de modo que:

1. La información se obtenga cumpliendo con cualquier legislación de protección de datos.

2. La entrada de información al sistema de publicación y su procesamiento se procese de manera oportuna.

3. La información sensible se proteja durante el proceso de recolección y cuando se almacene.

4. El acceso al sistema de publicación no permita el acceso involuntario a las redes con las cuales se conecte.

Otras formas de intercambio de información

Los procedimientos y los controles deben encontrarse en el lugar para proteger el intercambio de información mediante el uso de voz, del fax y de los medios de comunicación de video. La información puede comprometerse debido a la falta de alertas, política o procedimientos en el uso de tales instalaciones o medios – ser escuchado por casualidad en un teléfono celular en un lugar público, escuchar contestadoras automáticas por casualidad, el acceso no autorizado a los sistemas de correo de voz o accidentalmente enviar faxes a la persona incorrecta usando el equipo de fax.

Las operaciones de negocio pueden interrumpirse y la información comprometerse si las instalaciones o medios de comunicación fallan, también la información puede comprometerse si los usuarios no autorizados tienen acceso a ésta. Una política clara de procedimientos del personal debe establecerse para usar la voz, el fax y las comunicaciones de video. Esto debe incluir:

1. Recordar al personal que debe tomar precauciones apropiadas como no revelar información sensible para evitar ser escuchada por casualidad o interceptada al hacer una llamada telefónica por:

   - Personas en su vecindad inmediata particularmente al usar los teléfonos celulares.

   - Intercepción de mensajes telegráficos o telefónicos y otras formas de fisgoneo a través del acceso físico al equipo telefónico, a la línea telefónica, o usando receptores de exploración al usar teléfonos celulares análogos.

   - Gente en el extremo del receptor.

2. Recordar al personal que no debe tener conversaciones confidenciales en lugares públicos o en oficinas abiertas y lugares de reunión con paredes delgadas.

3. No dejar mensajes en las contestadoras automáticas, puesto que éstos pueden reproducirse por personas no autorizadas, almacenarse en sistemas comunales o almacenarse incorrectamente como resultado de una equivocación en el marcado.

4. Recordar al personal los problemas al usar las máquinas de fax:

   - Acceso no autorizado a los mensajes almacenados para recuperar mensajes.

   - Programación deliberada o accidental de las máquinas para enviar mensajes a números específicos.

   - Envío de documentos y mensajes a un número incorrecto debido a una marcación incorrecta o a un número almacenado incorrecto.

APÉNDICE G

CONTROL DE ACCESO

a) Requerimientos de negocio:

Política de control de acceso

Es conveniente definir y documentar los requerimientos del negocio para el control de acceso, también se deben indicar claramente en una política de control de acceso, las reglas y los derechos de control de acceso de cada usuario o grupo de usuarios – tanto los usuarios como los proveedores de servicio deben incluirse para ser considerados por los controles de acceso. La política debe tomar en cuenta lo siguiente:

1. Requerimientos de seguridad de las aplicaciones individuales de negocio.

2. Identificación de toda la información relacionada con las aplicaciones de negocio.

3. Políticas para la difusión y autorización de la información, por ejemplo, la necesidad de conocer principios y niveles de seguridad y clasificación de información.

4. Consistencia entre el control de acceso y las políticas de clasificación de la información de los diversos sistemas y redes.

5. Legislación relevante y obligaciones contractuales con respecto a la protección del acceso a los datos o a los servicios.

6. Perfiles estándares del acceso de usuarios para las categorías comunes del trabajo.

7. Administración de los derechos de acceso en un ambiente distribuido y de red que reconoce todos los tipos de conexiones disponibles.

Es importante que al especificar las reglas del control de acceso, se considere lo siguiente:

1. Distinguir entre las reglas que deben hacerse cumplir siempre y las reglas que son opcionales o condicionales.

2. Establecer reglas basadas en la premisa "Todo está prohibido excepto lo que está específicamente permitido" y no en la premisa "Todo lo que no esté específicamente prohibido está permitido".

3. Los cambios en las etiquetas de información que se realizan automáticamente por las instalaciones o medios de procesamiento de información y aquéllos que se realizan a discreción de un usuario.

4. Cambios en los permisos del usuario que se realizan automáticamente por el sistema de información y aquéllos realizados por un administrador.

5. Reglas que requieren la aprobación del administrador u otra aprobación antes de promulgase y las que no lo requieren.

b) Administración de usuario:

Registro del usuario

Es vital que exista un procedimiento formal de registro y eliminación del usuario para conceder el acceso a todos los sistemas y servicios multiusuarios de información, el acceso a los servicios informativos multiusuario debe controlarse mediante un proceso formal de registro del usuario, el cual considera:

1. Usar identificaciones de usuario únicas para poder hacerlo responsable de sus acciones. El uso de identificaciones de grupo debe permitirse donde sea conveniente para realizar trabajo en grupo.

2. Verificar que el usuario tiene autorización del dueño del sistema para usar la información o los servicios del sistema. Puede ser apropiada aprobación separada de los derechos de acceso de la administración.

3. Verificar que el nivel del acceso concedido es el apropiado para el propósito del negocio y consistente con la política de seguridad de la organización - no compromete la segregación de deberes.

4. Dar a los usuarios una declaración escrita de sus derechos de acceso.

5. Requerir que los usuarios firmen las declaraciones que indican que entienden las condiciones de acceso.

6. Asegurar que los proveedores del servicio no proporcionen el acceso hasta que se hayan completado los procedimientos de autorización.

7. Mantener un registro formal de todas las personas registradas para utilizar el servicio.

8. Inmediatamente remover los derechos de acceso de los usuarios que cambien de trabajo o dejen la organización.

9. Periódicamente comprobar y eliminar identificaciones y cuentas de usuario redundantes.

10. Asegurar que las identificaciones de usuario redundantes no se publiquen a otros usuarios.

Se deben incluir cláusulas en los contratos del personal y los contratos de servicio que especifiquen sanciones si el acceso no autorizado es realizado por los agentes del personal o del servicio. La asignación y el uso de privilegios (cualquier característica o facilidad de un sistema de información multiusuario que permite al usuario contrarrestar controles del sistema o de aplicación) deben restringirse y controlarse. El uso inadecuado de los privilegios del sistema es a menudo un factor importante que causa una falla en los sistemas.

Al sistema multiusuario que requiere la protección contra el acceso no autorizado se le debe asignar los privilegios controlados mediante un proceso formal de autorización. Los pasos siguientes deben considerarse:

1. Identificar los privilegios asociados a cada producto del sistema - el sistema operativo, administración de la base de datos y cada aplicación - y a las categorías del personal a las cuales necesitan asignarse.

2. Asignar los privilegios a los individuos sobre las bases: necesitar para usar, y evento por evento, es decir, sobre la base del requisito mínimo para su rol funcional solamente cuando es necesario.

3. Mantener un proceso de autorización y un registro de los privilegios asignados. Los privilegios no deben concederse hasta que el proceso de autorización se complete.

4. Promover el desarrollo y el uso de rutinas del sistema para evitar la necesidad de conceder privilegios a los usuarios.

5. Asignar los privilegios a una diversa identidad del usuario de ésos usados para el uso normal del negocio.

Administración de la contraseña del usuario

Las contraseñas son los medios comunes para validar una identidad de usuario y permitir el acceso a un sistema de información o a un servicio, la asignación de contraseñas debe controlarse mediante un proceso formal de administración, un acercamiento de esto:

1. Requerir que los usuarios firmen una declaración para mantener las contraseñas personales de manera confidencial y las contraseñas del grupo de trabajo solamente dentro de los miembros del grupo (esto se podría incluir en los términos y las condiciones del empleo).

2. Asegurar que los usuarios mantienen sus propias contraseñas, inicialmente se les proporciona una contraseña temporal segura, la cual deben cambiar inmediatamente. Las contraseñas temporales se proporcionan cuando los usuarios se olviden de su contraseña y se dan solamente cuando el usuario presente una identificación.

3. Dar contraseñas temporales requeridas a los usuarios de una manera segura. El uso de terceras entidades o mensajes desprotegidos de correo electrónico (texto claro) deben evitarse. Los usuarios deben reconocer cuando reciben contraseñas.

Las contraseñas nunca deben almacenarse en un sistema informático sin protección alguna, para eso se utilizan otras tecnologías para la identificación y la autenticación de usuario, como la biométrica - verificación de huella digital, verificación de firma – o las tarjetas con chip.

Para mantener el control eficaz del acceso a los datos y a los servicios de información, la administración debe realizar un proceso formal en intervalos regulares para revisar los derechos de acceso de los usuarios:

1. Los derechos de acceso se revisan en intervalos regulares (un período de 6 meses se recomienda) y después de cualquier cambio.

2. Las autorizaciones para derechos especiales de acceso privilegiado se deben revisar en intervalos más frecuentes; un período de 3 meses se recomienda.

3. Las asignaciones de privilegio se verifican en intervalos regulares para asegurar que los privilegios no autorizados no se han obtenido.

c) Responsabilidades del usuario:

Uso de la contraseña

Es indispensable que los usuarios sigan buenas prácticas de seguridad en la selección y el uso de contraseñas, pues éstas proporcionan medios para validar la identidad del usuario y establecen los derechos de acceso a las instalaciones o servicios de procesamiento de la información. A todos los usuarios se les debe aconsejar para:

1. Mantener las contraseñas confidenciales.

2. Evitar guardar papel como registro de contraseñas, a menos que esto se pueda almacenar con seguridad

3. Cambiar contraseñas siempre que haya cualquier indicación de que el sistema o la contraseña se han comprometido.

4. Seleccionar contraseñas de calidad con una longitud mínima de seis caracteres que sean:

   - Fáciles de recordar.

   - No basadas en cualquier persona que podría conjeturar u obtener fácilmente información de la persona que la utiliza - números de teléfono, nombres y fechas de nacimiento.

- Libre de caracteres idénticos consecutivos o de grupos completamente numéricos o alfabéticos.

5. Cambiar contraseñas en intervalos regulares o basarse en el número de accesos (las contraseñas para cuentas privilegiadas se deben cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización o viejas contraseñas.

6. Cambiar las contraseñas temporales en el primer inicio de sesión.

7. No incluir contraseñas en ningún proceso automatizado de conexión - almacenamiento en una macro o función clave.

8. No compartir contraseñas individuales de usuario.

Si los usuarios necesitan tener acceso a servicios múltiples o a plataformas y requieren tener múltiples contraseñas, es conveniente aconsejarlos para que utilicen una sola contraseña de calidad para todos los servicios.

Los usuarios deben asegurarse de que el equipo desatendido tenga protección apropiada. El equipo instalado en las áreas del usuario como sitios de trabajo o servidores de archivo, puede requerir protección específica contra el acceso no autorizado cuando se desatienda por un período largo. Todos los usuarios y contratistas deben enterarse de los requerimientos y de los procedimientos de seguridad para proteger el equipo desatendido, así como sus responsabilidades para implementar tal protección. Los usuarios deben aconsejarse para:

1. Terminar sesiones activas cuando hayan acabado, a menos que éstas puedan asegurarse mediante un mecanismo de cierre apropiado, por ejemplo, un protector de pantallas protegido con contraseña.

2. Salir de sesión cuando se termina de usar el equipo (es decir, no sólo apagar la PC o la terminal).

3. Asegurar las computadoras personales o las terminales de aplicación no autorizada mediante un bloqueo de teclas o un control equivalente - acceso con contraseña.

d) **Control de acceso en la red:** debe controlarse el acceso a los servicios en red internos y externos, esto es necesario para asegurar que los usuarios que tienen acceso a las redes y a los servicios de red no comprometen la seguridad de estos servicios de red, para esto se necesitan:

1. Interfaces apropiadas entre la red de la organización y las redes de otras organizaciones, o redes públicas.

2. Mecanismos apropiados de autenticación para los usuarios y el equipo.

3. Control de acceso del usuario a los servicios de información.

Política en el uso de los servicios de red

Las conexiones inseguras a los servicios de red pueden afectar a la organización entera. A los usuarios se les debe proporcionar solamente el acceso directo a los servicios para los que han sido autorizados específicamente, este control es particularmente importante para las conexiones de red a las aplicaciones de negocio sensibles o críticas o a los usuarios en áreas de riesgo elevado - las áreas públicas o externas que están fuera de la administración y control de seguridad de la organización. Una política se debe formular referente al uso de redes y servicios de red, por lo tanto debe cubrir:

1. Las redes y los servicios de red a los que se permite tener acceso.

2. Procedimientos de autorización para determinar a quién se les permite el acceso y a qué redes y servicios.

3. Controles y procedimientos de administración para proteger el acceso a las conexiones de red y a los servicios de red.

Esta política debe ser consistente con la política de control de acceso del negocio.

La ruta desde la terminal del usuario hasta el servicio de cómputo debe controlarse. Las redes se diseñan para permitir al máximo la posibilidad de compartir los recursos y la flexibilidad de encaminamiento, estas características proporcionan oportunidades para el acceso no autorizado a las aplicaciones de negocio o el uso no autorizado de las instalaciones o

medios de información, sin embargo, si se incorporan controles que restringen la ruta entre una terminal de usuario y los servicios informáticos a los que el usuario está autorizado a tener acceso - creando una ruta obligada - puede reducir tales riesgos. El objetivo de una trayectoria obligada es prevenir que cualquier usuario seleccione rutas fuera de la ruta entre la terminal del usuario y los servicios a los que el usuario está autorizado para acceder, lo anterior requiere generalmente la puesta en práctica de controles en diversos puntos de la ruta. El objetivo es limitar las opciones de ruta en cada punto de la red mediante opciones predefinidas. Ejemplos de esto:

1. Asignación dedicada de líneas o números de teléfono.

2. Automáticamente conectar puertos con aplicaciones específicas del sistema o puertas de seguridad.

3. Limitación de las opciones del menú y del submenú para los usuarios individuales.

4. Prevención de la red ilimitada.

5. Hacer cumplir el uso de las aplicaciones específicas de los sistemas y/o de las puertas de seguridad para los usuarios externos de la red.

6. Activamente controlar la fuente que se permite como destino de las comunicaciones vía puertas de seguridad, por ejemplo, firewalls.

7. Restringir el acceso a la red colocando dominios lógicos separados - redes privadas virtuales - para grupos de usuario dentro de la organización.

Los requerimientos para una ruta obligada se deben basar en la política de control de acceso del negocio.

Autenticación del usuario para conexiones externas

Las conexiones externas proporcionan un potencial para el acceso no autorizado a la información del negocio, un ejemplo es el acceso por métodos de marcado manual. Por lo tanto, el acceso de los usuarios remotos debe estar sujeto a la autenticación. Existen diversos tipos de

método de autenticación, algunos de ellos proporcionan un mayor nivel de protección que otros, por ejemplo, los métodos basados en el uso de técnicas criptográficas pueden proporcionar autenticación fuerte. Es importante determinar mediante una evaluación de riesgo el nivel de protección requerido, esto es necesario para seleccionar apropiadamente un método de autenticación. La autenticación de usuarios remotos puede lograrse usando, por ejemplo, una técnica criptográfica o un protocolo de llegada/respuesta. Es posible utilizar líneas privadas dedicadas o un medio de comprobación de dirección del usuario de red para proporcionar el aseguramiento de la fuente de conexiones. Los procedimientos y los controles de marcado - módems de marcado - proporcionan protección contra conexiones no autorizadas e indeseadas a las instalaciones de procesamiento de información de la organización, este tipo de control autentica a los usuarios que intentan establecer una conexión a la red de la organización desde posiciones remotas; al usar este control, una organización no debe utilizar los servicios de red que incluyen la expedición o, si lo hacen, deben deshabilitar el uso de tales características para evitar las debilidades asociadas a la expedición de llamadas. Es importante que el proceso de retiro incluya el aseguramiento de que ocurre una desconexión real del lado de la organización, si no, el usuario remoto podría mantener abierta la conexión y fingir que ocurre su retiro. Los procedimientos de retiro y los controles se deben probar a fondo para evitar esta posibilidad.

Una forma de conexión automática a una computadora remota también puede proporcionar una manera de acceso no autorizado a una aplicación de negocio, las conexiones al sistema informático remoto deben, por lo tanto, autenticarse; esto es especialmente importante si la conexión utiliza una red que esté fuera del control de la administración de seguridad de la organización. La autenticación del nodo puede servir como un medio alternativo para autenticar a grupos de usuarios remotos que estén conectados con una instalación informática segura y compartida.

El acceso a los puertos de diagnóstico debe controlarse con seguridad. Muchas computadoras y sistemas de comunicación se instalan con la facilidad para realizar un diagnóstico remoto de marcado manual y así ser utilizado por los ingenieros de mantenimiento. Si se descuidan, estos puertos de diagnóstico proporcionan medios de acceso no autorizado, por lo tanto, deben protegerse mediante un mecanismo apropiado de seguridad, por ejemplo, un bloqueo y un procedimiento para asegurar que

son solamente accesibles mediante el arreglo entre el encargado del servicio y el personal de soporte de hardware y software que requiere el acceso.

Segregación en redes

Las redes se extienden cada vez más allá de los límites de la organización, pues se forman sociedades de negocio que pueden requerir la interconexión o la posibilidad de compartir las instalaciones de procesamiento de información, tal extensión puede aumentar el riesgo de acceso no autorizado a los sistemas de información ya existentes que utilizan la red, algo de la cual puede requerir la protección contra otros usuarios de la red debido a su sensibilidad. En tales circunstancias, debe considerarse la introducción de controles dentro de la red para segregar grupos de servicios de información, usuarios y sistemas de información. Un método para controlar la seguridad de las grandes redes es dividirlas en dominios lógicos de red separados - dominios internos de una red de la organización y dominios externos de la red, cada uno protegido por un perímetro definido de seguridad, tal perímetro puede implementarse instalando una puerta segura entre las dos redes que se interconectan para controlar el acceso y el flujo de información entre los dos dominios, la puerta debe configurarse para filtrar tráfico entre esos dominios y para bloquear el acceso no autorizado con base en la política de control de acceso de la organización; un ejemplo de este tipo de entrada el firewall. Los criterios para la segregación de redes en dominios deben basarse en la política de control de acceso y en los requerimientos de acceso, y también tomar en cuenta el costo y el impacto relativos al incorporar tecnología conveniente para el encaminamiento de la red o la entrada a la red.

Control de la red

Los requerimientos de la política de control de acceso para las redes compartidas, especialmente ésas que se extienden a través de los límites de la organización pueden requerir la incorporación de controles para restringir la capacidad de conexión de los usuarios, tales controles se pueden implementar a través de las entradas de la red que filtran el tráfico por medio de tablas o reglas predefinidas. Las restricciones aplicadas deben basarse en la política de acceso y en los requerimientos de las aplicaciones de negocio, también se deben mantener y poner al día. Las restricciones deben aplicarse a:

1. Correo electrónico.

2. Transferencia unidireccional de archivo.

3. Transferencia bidireccional de archivo.

4. Acceso interactivo.

5. Acceso a la red ligado a la hora o a la fecha.

Las redes compartidas, especialmente ésas que se extienden a través de los límites de la organización, pueden requerir la incorporación de controles de encaminamiento para asegurar que las conexiones de la computadora y los flujos de información no provoquen una brecha en la política de control de acceso de las aplicaciones del negocio. Este control es a menudo esencial para las redes que se comparten con los usuarios de terceras entidades. Los controles de encaminamiento deben basarse en mecanismos que comprueben la dirección de la fuente y el destino. La conversión de la dirección de red es también un mecanismo muy útil para aislar redes y prevenir rutas de propagación entre la red de una organización y otra, los controles pueden implementarse en software o hardware. Los servicios de red pueden tener características únicas o complejas de seguridad, por lo que las organizaciones que usan servicios de red deben asegurarse de que una descripción clara de las cualidades de seguridad de todos los servicios usados se proporcione.

e) **Control de acceso del sistema operativo:** las instalaciones o medios de seguridad a nivel del sistema operativo se deben utilizar para restringir el acceso a los recursos de la computadora. Estas instalaciones o medios deben ser capaces de lo siguiente:

1. Identificar y verificar la identidad, y si es necesario, la terminal o la localización de cada usuario autorizado.

2. Registrar accesos al sistema exitosos y fallidos.

3. Proveer medios apropiados para la autenticación; si se utiliza un sistema de administración de contraseña, debe asegurar contraseñas de calidad.

4. Cuando sea apropiado, restringir los tiempos de conexión de los usuarios.

Debe considerarse la identificación automática de la terminal para autenticar conexiones a lugares específicos y a un equipo portátil. La identificación automática de la terminal es una técnica que puede utilizarse si es importante que la sesión se pueda iniciar solamente desde una localización o de una terminal particular. Un identificador en la terminal o adjunto a ésta se puede utilizar para indicar si a esta terminal particular se le permite iniciar o recibir transacciones específicas. Puede ser necesario aplicar una protección física a la terminal para mantener la seguridad del identificador de la terminal.

El acceso a los servicios de información debe alcanzarse vía un proceso seguro de conexión. Debe diseñarse un procedimiento para iniciar sesión o conectarse a un sistema informático y reducir al mínimo la oportunidad de acceso no autorizado. El procedimiento de conexión debe, por lo tanto, divulgar al mínimo información sobre el sistema para evitar proveerle a un usuario no autorizado la ayuda necesaria. Un buen procedimiento de conexión o inicio de sesión debe:

1. Evitar desplegar identificadores del sistema o de la aplicación hasta que el proceso de conexión se haya terminado con éxito.

2. Desplegar un aviso de advertencia general de que la computadora permitirá el acceso solamente a los usuarios autorizados.

3. Evitar proporcionar mensajes de ayuda durante el procedimiento de conexión que ayudaría a un usuario no autorizado.

4. Validar la información de conexión a la comunicación solamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.

5. Limitar el número de intentos fallidos permitidos de conexión (se recomienda tres) y considerar:

   - Registrar intentos fallidos.

- Forzar un retraso antes de que nuevos intentos de conexión se permitan o rechazar intentos futuros sin autorización específica.

- Desconectar conexiones de transmisión de datos.

6. Limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión. Si se excede, el sistema debe terminar la conexión.

7. Desplegar la información siguiente cuando se complete exitosamente la conexión:

   - Fecha y hora de la conexión anterior.

   - Detalles de cualquier intento fallido de conexión desde la última conexión exitosa.

Identificación y autenticación de usuario

Todos los usuarios (incluyendo al personal de soporte técnico, tal como operadores, administradores de la red, programadores y administradores de la base de datos) deben tener un identificador único (identificación del usuario) para su uso personal y único, de tal manera que las actividades se le señalen al individuo responsable. Las identificaciones de usuario no deben dar ninguna indicación del nivel de privilegio del usuario, por ejemplo, encargado, supervisor. En circunstancias excepcionales, donde existe un beneficio claro del negocio, puede utilizarse el uso de una identificación de usuario que se comparte con un grupo de usuarios o un trabajo específico, sin embargo, es indispensable que exista la aprobación de la administración, la cual debe documentarse para tales casos. Algunos controles adicionales pueden requerirse para mantener la responsabilidad. Hay varios procedimientos de autenticación que pueden utilizarse para verificar la identidad demandada de un usuario, las contraseñas son una manera muy común para proporcionar la identificación y la autenticación con base en un secreto que solamente el usuario sabe. También se pueden utilizar medios y protocolos criptográficos de autenticación. Objetos tales como muestras de memoria o tarjetas inteligentes que los usuarios poseen se pueden utilizar para identificar y autenticar o las tecnologías biométricas de autenticación que utilizan las características o las cualidades únicas de un individuo también se usan para comprobar la

identidad de la persona. Una combinación de tecnologías y mecanismos ligados con la seguridad dará lugar a una autenticación más fuerte.

Las contraseñas son uno de los medios principales para validar la autoridad de un usuario para tener acceso a un servicio de información, por lo que es indispensable que los sistemas de administración de contraseña proporcionen un medio eficaz e interactivo que asegure contraseñas de calidad. Algunas aplicaciones requieren que las contraseñas del usuario sean asignadas por una autoridad independiente, aunque en la mayoría de los casos los usuarios seleccionan y mantienen las contraseñas. Un buen sistema de administración de contraseña debe:

1. Forzar el uso de contraseñas individuales para mantener la responsabilidad.

2. Cuando sea apropiado, permitir que los usuarios seleccionen y que cambien sus propias contraseñas y que exista un procedimiento de confirmación en caso de que se presenten errores.

3. Forzar a tener contraseñas de calidad.

4. Cuando los usuarios mantienen sus propias contraseñas, cambiar la contraseña regularmente.

5. Cuando los usuarios seleccionen contraseñas, forzarlos a cambiar contraseñas temporales en la primera conexión.

6. Mantener un registro de las contraseñas anteriores del usuario, por ejemplo, las de 12 meses anteriores, y prevenir la reutilización.

7. No exhibir contraseñas en la pantalla al ser escritas.

8. Almacenar archivos de contraseña separados de los datos de las aplicaciones del sistema.

9. Almacenar contraseñas en forma cifrada usando un algoritmo unidireccional de cifrado.

10. Alterar las contraseñas por defecto del vendedor después de la instalación del software.

Uso de las utilidades del sistema

La mayoría de las computadoras tienen uno o más programas de utilidades del sistema que pueden ser capaces de rechazar los controles del sistema y de las aplicaciones. Es esencial que su uso se restrinja y se controle firmemente. Los controles siguientes deben considerarse:

1. Uso de procedimientos de autenticación para las utilidades del sistema.

2. Segregación de las utilidades del sistema del software de aplicaciones.

3. Limitaciones en el uso de las utilidades del sistema a un número mínimo confiable de usuarios autorizados.

4. Autorización para el uso ad hoc de las utilidades del sistema.

5. Limitación de la disponibilidad de las utilidades del sistema, por ejemplo, para la duración de un cambio autorizado.

6. Conexión a todo el uso de las utilidades del sistema.

7. Definir y documentar los niveles de autorización de las utilidades del sistema.

8. Retiro de todo el software innecesario basado en las utilidades y software del sistema.

La disposición de una alarma de compulsión[33] debe considerarse para los usuarios que pueden ser blancos de la coacción[34]. La decisión para proveer tal alarma debe basarse en una evaluación de riesgos. Deben existir responsabilidades y procedimientos definidos para responder a una alarma de compulsión.

Las terminales inactivas en lugares de alto riesgo - áreas públicas o externas y fuera de la administración de seguridad de la organización -, deben apagarse después de un período definido de inactividad para

[33] Obligar a uno legalmente a que haga una cosa.
[34] Violencia que se hace a alguno para que ejecute una cosa contra su voluntad.

prevenir el acceso de las personas no autorizadas, este medio de apagado debe limpiar la pantalla de la terminal y cerrar las sesiones de trabajo y de la red después de un período definido de inactividad. Una forma limitada del medio de apagado de la terminal se puede proporcionar para algunas PC que limpian la pantalla y previenen el acceso no autorizado, pero que no cierran las sesiones de trabajo o de red.

Las restricciones en los tiempos de conexión deben proporcionar seguridad adicional para las aplicaciones de riesgo elevado. La limitación del período durante el cual a las conexiones terminales se les permite el acceso a los servicios de información reduce las oportunidades para el acceso no autorizado, tal control debe considerarse para aquellas aplicaciones informáticas sensibles, especialmente ésas con terminales instaladas en lugares de alto riesgo - áreas públicas o externas que están fuera de la administración de la seguridad de la organización. Ejemplos de tales restricciones incluyen:

1. Uso de canales de tiempo predeterminado - para las transmisiones de archivo o sesiones interactivas regulares de duración corta.

2. Restricción de tiempos de conexión a las horas de oficina normales, si no hay requisito para tiempo suplementario, o extender horas de operación.

f) **Aplicación del control de acceso:** las aplicaciones del sistema deben:

1. Establecer que el control de acceso del usuario a la información y a las aplicaciones del sistema funciona, de acuerdo con una política definida de control de acceso del negocio.

2. Proveer protección contra el acceso no autorizado a cualquier software de utilidad y de sistema operativo que sea capaz de eliminar controles del sistema o de aplicación.

3. No comprometer la seguridad de otros sistemas con los cuales se comparten los recursos de la información.

4. Ser capaz de proporcionar el acceso a la información al dueño solamente, o a otros individuos que se autoricen, o a grupos definidos de usuarios.

A los usuarios de las aplicaciones del sistema, incluyendo el personal de soporte, se les debe proveer el acceso a la información y a funciones de las aplicaciones del sistema de acuerdo con una política definida de control de acceso, basada en requerimientos individuales de aplicación de negocio y consistente con la política de acceso a la información de la organización. Es importante considerar la aplicación de los controles siguientes para apoyar los requerimientos de la restricción del acceso:

1. Proporcionar menús para el control de acceso a las funciones de aplicación del sistema.

2. Restringir el conocimiento de información o funciones de aplicación del sistema, a los usuarios que no se les autoriza el acceso, con base en una documentación apropiada.

3. Controlar los derechos de acceso de los usuarios, leer, escribir, borrar y ejecutar.

4. Asegurar que las salidas de las aplicaciones del sistema que manejen la información sensible contienen solamente la información que es relevante para su uso en la salida y se envían solamente a las terminales y a los lugares autorizados, incluyendo la revisión periódica de tales salidas para asegurar que la información redundante se elimina.

Los sistemas sensibles pueden requerir un ambiente de cómputo (aislado) dedicado. Algunas aplicaciones de los sistemas son suficientemente sensibles a la pérdida potencial que requieren un manejo especial. La sensibilidad puede indicar que la aplicación del sistema debe funcionar en una computadora dedicada, debe compartir solamente recursos con las aplicaciones del sistema confiables, o no tener ninguna limitación. Es vital aplicar las consideraciones siguientes:

1. La sensibilidad de una aplicación del sistema debe identificarse y documentarse explícitamente por el dueño de aplicación.

2. Cuando una aplicación sensible funciona en un ambiente compartido, las aplicaciones de los sistemas con los cuales compartirá recursos deben identificarse y convenirse con el dueño de la aplicación sensible.

g) **Supervisión de acceso:** los registros de inicio de sesión guardan excepciones y otros acontecimientos de seguridad relevantes que se producen y éstos deben guardarse por un período convenido para ayudar a futuras investigaciones y supervisiones del control de acceso. Los registros de inicio de sesión deben también incluir:

1. Identificaciones de usuario.
2. Fechas y tiempos de conexión y desconexión.
3. Identidad o lugar de la terminal si es posible.
4. Registro de intentos de acceso al sistema exitosos y fallidos.
5. Registros de acceso a datos exitosos y fallidos y de otros intentos de acceso a recursos.

Ciertos registros de conexión pueden requerirse para archivarse como parte de la política de registro de retención o debido a requerimientos para recolectar evidencia.

Uso de supervisión del sistema

Es importante establecer procedimientos para supervisar el uso de las instalaciones o medios de procesamiento de la información, tales procedimientos son necesarios para asegurar que los usuarios realicen solamente las actividades que se les ha autorizado explícitamente. El nivel de supervisión requerido para las instalaciones o medios individuales se debe determinar mediante una evaluación de riesgo. Las áreas que deben considerarse incluyen:

1. Acceso autorizado, incluyendo a detalle:
   - Identificación del usuario.
   - Fecha y hora de los eventos claves.
   - Tipos de eventos.
   - Archivos que tuvieron acceso.

- Programas y utilidades utilizados.

2. Todas las operaciones privilegiadas, por ejemplo:

   - Uso de la cuenta del supervisor.
   - Arrancar y parar el sistema.
   - Adjuntar y eliminar dispositivos de entrada/salida.

3. Intentos de acceso no autorizado, por ejemplo:

   - Intentos fallidos.
   - Violaciones a la política de acceso y notificaciones de entrada a la red y firewalls.
   - Alertas de sistemas propietarios de detección de intrusos.

4. Alertas o fallas del sistema, por ejemplo:

   - Alertas o mensajes de la consola.
   - Excepciones del registro del sistema.
   - Alertas de administración de la red.

El resultado de las actividades de supervisión debe revisarse regularmente. La frecuencia de la revisión depende de los riesgos implicados. Los factores de riesgo que es necesario considerar incluyen:

1. Qué tan críticos son los procesos de aplicación.
2. El valor, la sensibilidad o lo crítico de la información implicada.
3. La experiencia previa de la infiltración y mal uso del sistema.
4. El grado de interconexión del sistema (particularmente redes públicas).

Una revisión de la conexión implica entender las amenazas enfrentadas por el sistema y de qué manera éstas pueden presentarse. Los registros del sistema contienen a menudo un gran volumen de información, mucho del cual es extraño para la supervisión de la seguridad. Para ayudar a identificar los acontecimientos significativos para propósitos de supervisión de la seguridad, es conveniente considerar el copiado de los mensajes apropiados de forma automática a un segundo registro, y/o el uso de utilidades convenientes del sistema o herramientas de revisión para realizar la investigación del archivo. Al asignar la responsabilidad de la revisión del registro, una separación de papeles se lleva a cabo entre la o las personas que realizan la revisión y aquéllas a las que se les supervisa las actividades. Los controles deben proteger contra cambios no autorizados y problemas operacionales, esto incluye:

1. Los medios de conexión si se desactivan.

2. Alteraciones a los mensajes que se registran.

3. Archivos de registro que se editan o suprimen.

4. Medios de archivos de registros que se agotan y no pueden registrar acontecimientos o aquéllos que se sobrescriben.

Es importante realizar un ajuste correcto de los relojes de la computadora para asegurar la exactitud de los registros, pues éstos se pueden requerir para investigaciones o como evidencia en casos legales o disciplinarios. Los registros inexactos pueden obstaculizar las investigaciones y dañar la credibilidad de tal evidencia. Cuando una computadora o un dispositivo de comunicación tiene la capacidad para hacer funcionar un reloj en tiempo real, debe fijarse a un estándar convenido como el tiempo coordinado universal (UCT) o un tiempo estándar local, ya que algunos relojes se modifican con el tiempo, es esencial que exista un procedimiento que compruebe y corrija cualquier variación significativa.

h) Cómputo móvil: es indispensable tener cuidado al usar medios móviles de cómputo - notebooks, palmtops, laptops y teléfonos celulares -, para evitar que la información del negocio se comprometa, para esto, debe adoptarse una política formal que considere los riesgos que se presentan al trabajar con medios móviles de cómputo, sobre todo en ambientes desprotegidos.

Por ejemplo, tal política debe incluir requerimientos para la protección física, los controles de acceso, técnicas criptográficas, respaldos, y protección contra virus. Esta política también debe incluir reglas y consejos sobre la conexión de medios móviles con las redes y la manera de utilizarlos en lugares públicos. Es conveniente tener cuidado al usar medios móviles de cómputo en lugares públicos, cuartos de reunión y otras áreas desprotegidas que se encuentren fuera de las instalaciones de la organización, esta protección debe evitar el acceso no autorizado o la divulgación de información almacenada y procesada por estas instalaciones o medios, para ello, se hace uso de técnicas criptográficas. Es importante que cuando tales medios se utilicen en lugares públicos se evite el riesgo de uso por personas no autorizadas.

Los procedimientos contra el software malicioso deben encontrarse en el lugar y aplicarse continuamente. Es vital que el equipo se encuentre disponible para permitir el respaldo rápido y fácil de la información, a estos respaldos se les debe brindar una protección adecuada contra el robo o la pérdida de información. Otra consideración de suma importancia, es la protección conveniente que debe darse al uso de los medios móviles conectados a las redes, pues el acceso remoto a la información del negocio a través de la red pública que usa medios de cómputo móvil debe ocurrir solamente después de la identificación y de la autenticación exitosas y con base en mecanismos convenientes de control de acceso en el lugar.

Los medios móviles de cómputo deben protegerse físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, cuartos de hotel, centros de conferencia y lugares de reunión. El equipo que contiene información importante, sensible y/o crítica del negocio, no debe desatenderse y, en lo posible, es esencial poner bajo llave o colocar candados que lo aseguren. Todo el personal que usa cómputo móvil debe entrenarse para conocer los riesgos adicionales que pueden presentarse como resultado de esta forma del trabajo y los controles que deben implementarse.

Las telecomunicaciones utilizan tecnología de punta en comunicaciones para permitir al personal trabajar remotamente en un lugar fijo fuera de su organización, por lo tanto, es conveniente proteger este sitio de trabajo para evitar el robo del equipo y la información, la divulgación no autorizada de la información, el acceso remoto no autorizado a los sistemas de la organización o el mal uso de los medios. Es importante que

la administración autorice y controle las telecomunicaciones y que se encuentren en el lugar de trabajo las características necesarias para su uso. Las organizaciones deben considerar el desarrollo de una política, procedimientos y estándares para controlar las actividades de telecomunicaciones, también deben autorizar actividades de telecomunicaciones si se satisfacen las características y controles apropiados de seguridad en el lugar y que éstos cumplan con la política de seguridad de la organización. A continuación se listan puntos que deben tomarse en cuenta:

1. La seguridad física existente en el sitio de trabajo, considerando la seguridad física del edificio y del ambiente local.

2. El ambiente propuesto de telecomunicaciones.

3. Los requerimientos de seguridad de las comunicaciones, considerando la necesidad del acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tiene acceso y se transmite a través de la liga de comunicaciones y la sensibilidad del sistema interno.

4. La amenaza del acceso no autorizado a la información o a los recursos mediante otras personas que usan sus relaciones, por ejemplo, familia y amigos.

Los controles y las acciones que se considerarán incluyen:

1. La disposición de equipo y de los muebles convenientes de almacenamiento para las actividades de trabajo remoto y las telecomunicaciones.

2. Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede obtener y los sistemas y servicios internos a los que el trabajador remoto puede tener acceso.

3. La disposición del equipo de comunicación conveniente incluyendo los métodos para asegurar el acceso remoto.

4. Seguridad física.

5. Reglas y guía para el acceso de la familia y el visitante al equipo y a la información.

6. Disposición de soporte y mantenimiento de hardware y software.

7. Procedimientos para la continuidad del respaldo y del negocio.

8. Intervención y supervisión de la seguridad.

9. Revocación de la autoridad, derechos de acceso y regreso del equipo, cuando las actividades del trabajo remoto y telecomunicaciones cesen.

APÉNDICE H

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

a) **Requerimientos de seguridad del sistema:** las declaraciones de los requerimientos del negocio para los nuevos sistemas, o los realces a los sistemas existentes, deben especificar los requerimientos necesarios para los controles, tales especificaciones deben considerar los controles automatizados que deben incorporarse al sistema, y la necesidad de apoyar controles manuales, consideraciones similares deben aplicarse al evaluar los paquetes de software para las aplicaciones de negocio. Si se considera apropiado, la administración puede hacer uso de productos independientemente evaluados y certificados. Los requerimientos y los controles de seguridad deben reflejar el valor para el negocio de los activos de información implicados, y el daño potencial al negocio que puede resultar debido a una falla o ausencia de seguridad. El marco para analizar requerimientos de seguridad e identificar los controles para satisfacerlos es la evaluación de riesgo y el manejo del riesgo, los controles que se introducen en la etapa de diseño son perceptiblemente más baratos para implementar y mantener que ésos incluidos durante o después de la puesta en práctica.

b) **Requerimientos de la seguridad de la aplicación:**

Validación de datos de entrada

La entrada de datos a los sistemas de aplicación debe validarse para asegurar que ésta es correcta y apropiada, por lo tanto, debe aplicarse una verificación a la entrada de las transacciones de negocio, los datos que permanecen (nombres, direcciones, límites de crédito, números de referencia del cliente) y tablas de parámetro (precios de venta, índices de conversión de monedas, rangos de impuestos). Los controles siguientes deben considerarse:

1. Entrada dual u otra verificación de entrada para detectar los errores siguientes:

   - Valores fuera de rango.
   - Caracteres inválidos en campos de datos.
   - Datos incompletos o faltantes.

- Exceder los límites superiores e inferiores del volumen de los datos.

- Control de datos no autorizados o inconsistente.

2. Revisión periódica del contenido de los campos claves o de los archivos de datos para confirmar su validez e integridad.

3. Inspección de documentos de entrada para evitar cualquier cambio no autorizado a los datos de entrada (todos los cambios a los documentos de entrada deben autorizarse).

4. Procedimientos para responder a los errores de validación.

5. Procedimientos para probar la credibilidad de los datos de entrada.

6. Definición de responsabilidades de todo el personal implicado en el proceso de entrada de datos.

Control del procesamiento interno

Los datos que entran correctamente pueden corromperse debido a errores de proceso o mediante actos deliberados, es por esto, que conviene la incorporación de pruebas de validación en los sistemas para detectar tal corrupción. El diseño de aplicaciones debe asegurar que se implementen restricciones para reducir al mínimo el riesgo en los medios de procesamiento que conducen a una pérdida de integridad. Las áreas específicas a considerar incluyen:

1. El uso y la ubicación en programas de funciones para agregar y suprimir, que implementen cambios en los datos.

2. Los procedimientos para prevenir que los programas funcionen de manera incorrecta o después de una falla del proceso anterior.

3. El uso de programas correctos para recuperarse de fallas y asegurar el procesamiento correcto de los datos.

Los controles que se requieren dependen de la naturaleza de la aplicación y del impacto en el negocio si se presenta cualquier corrupción de datos. Ejemplos de pruebas que pueden incorporarse incluyen:

1. Controles de sesión o de recibo/envío para ajustar los balances de los archivos de datos después de la actualización de la transacción.

2. Controles de balanceo para verificar los balances abiertos contra los balances cerrados anteriores, a saber:

   - Controles ejecución a ejecución.

   - Archivo de actualizaciones totales.

   - Controles programa a programa.

3. Validación de datos generados por el sistema.

4. Pruebas en la integridad de los datos o del software descargado o cargado entre las computadoras centrales y las remotas.

5. Identificación total de registros y archivos.

6. Pruebas para asegurar que los programas de aplicación estén funcionados en el momento correcto.

7. Pruebas para asegurar que los programas estén funcionados en el orden correcto y que terminan en caso de que exista una falla, y que el proceso posterior se detenga hasta que se resuelve el problema.

Autenticación del mensaje

La autenticación del mensaje es una técnica que se utiliza para detectar cambios no autorizados, o corrupción del contenido de un mensaje electrónico transmitido, puede implementarse en el hardware o el software mediante un dispositivo físico de autenticación del mensaje o un algoritmo del software. La autenticación del mensaje debe considerarse para las aplicaciones donde existe un requerimiento de seguridad para proteger la integridad del contenido de un mensaje, por ejemplo, transferencia electrónica de fondos, especificaciones, contratos, ofertas, con una

importancia alta u otros intercambios de datos electrónicos similares. Es indispensable realizar una evaluación de los riesgos de seguridad para determinar si se requiere la autenticación del mensaje y para identificar el método más apropiado de implementación. La autenticación del mensaje no se diseña para proteger el contenido de un mensaje contra la divulgación no autorizada. Las técnicas criptográficas se pueden utilizar como medios apropiados para implementar la autenticación del mensaje.

Validación de datos de salida

La salida de datos de una aplicación del sistema debe validarse para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias. Típicamente, los sistemas se construyen bajo la premisa de que han sido validados, verificados y probados, de esta manera los datos de salida serán siempre correctos, sin embargo, éste no es siempre el caso. La validación de la salida puede incluir:

1. Las pruebas de credibilidad se realizan para probar si los datos de la salida son razonables.

2. Cuentas del control de conformidad para asegurar el proceso de todos los datos.

3. Abastecimiento de suficiente información para un lector o un sistema de procesamiento subsecuente para determinar la exactitud, la precisión y la clasificación de la información y que ésta esté completa.

4. Procedimientos para responder a las pruebas de validación de la salida.

5. Definir las responsabilidades de todo el personal implicado en el proceso de la salida de datos.

c) **Criptografía:** tomar la decisión de si una solución criptográfica es apropiada es parte de un proceso más amplio de evaluación de riesgos y selección de controles, una evaluación de riesgo debe realizarse para determinar el nivel de protección que se le da a la información. Esta evaluación se puede utilizar para determinar si un control criptográfico es apropiado, qué tipo de control debe aplicarse y para qué procesos y propósitos del negocio. Es trascendental que una organización desarrolle una política para el uso de los controles criptográficos en la protección de

su información, en tal política, es necesario maximizar ventajas, reducir al mínimo los riesgos por usar técnicas criptográficas y evitar el uso inadecuado o incorrecto. Al desarrollar una política lo que sigue debe considerarse:

1. La administración del uso de controles criptográficos en la organización, incluyendo los principios generales bajo los cuales la información del negocio debe protegerse.

2. La administración de las claves, incluyendo métodos que traten con la recuperación de la información cifrada en caso de claves perdidas, comprometidas o dañadas.

3. Papeles y responsabilidades, por ejemplo, quién es el responsable para...

4. Implementación de la política.

5. Administración de claves.

6. Cómo determinar el nivel apropiado de protección criptográfica.

7. Estándares que se adoptarán para la puesta en práctica eficaz en la organización (qué solución se utiliza para qué proceso de negocio).

Cifrado

El cifrado es una técnica criptográfica que se puede utilizar para proteger la confidencialidad de la información, ésta debe considerarse para proteger la información sensible o crítica; con base en una evaluación de riesgo, se identifica el nivel requerido de protección, considerando el tipo y la calidad del algoritmo de cifrado a utilizar y la longitud de las claves criptográficas que se utilizarán. Al implementar la política criptográfica de la organización, se deben considerar las regulaciones y las restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas en diversas partes del mundo y a las aplicaciones para transportar el flujo de la información cifrada, además, se deben considerar los controles que se aplican a la exportación y a la importación de tecnología criptográfica. Se debe tomar en cuenta el consejo del especialista para identificar el nivel apropiado de protección, para seleccionar los productos convenientes que

proporcionarán la protección requerida y la puesta en práctica de un sistema seguro de la administración de claves, siempre es importante buscar asesoramiento jurídico para respetar las leyes y las regulaciones que pueden aplicarse al uso previsto de cifrado de la organización.

Firmas digitales

Las firmas digitales proporcionan medios para proteger la autenticidad y la integridad de documentos electrónicos, por ejemplo, pueden utilizarse en comercio electrónico donde existe la necesidad de verificar quién firmó un documento electrónico y si el contenido del documento firmado se ha cambiado. Las firmas digitales pueden aplicarse a cualquier forma de documento que se procesa electrónicamente - pueden ser utilizadas para firmar pagos electrónicos, transferencias de fondos, contratos y acuerdos. Las firmas digitales se implementan usando una técnica criptográfica basada en un único y relacionado par de claves, donde una clave se utiliza para crear una firma (la clave privada) y la otra para comprobar la firma (la clave pública), es sumamente importante proteger la confidencialidad de la clave privada. Esta clave debe mantenerse secreta ya que cualquier persona que tenga acceso a esta clave puede firmar documentos – pagos, contratos -, pues se convierte en la firma del dueño de esa clave. La protección de la integridad de la clave pública es importante, esta protección se proporciona mediante el uso de un certificado de clave pública.

Es esencial considerar el tipo y la calidad del algoritmo de firma que se emplea y la longitud de las claves que se utilizan. Las claves criptográficas usadas para las firmas digitales deben ser diferentes a las utilizadas para el cifrado. Al emplear firmas digitales, es necesario tomar en cuenta a la legislación relevante que describe las condiciones bajo las cuales una firma digital es legal, por ejemplo, en el caso del comercio electrónico es importante saber la situación legal de las firmas digitales. Puede ser necesario tener contratos obligatorios u otros acuerdos para apoyar el uso de firmas digitales donde es inadecuado el marco jurídico, aun así, debe buscarse el asesoramiento jurídico, respetando las leyes y las regulaciones que pueden aplicarse si la organización desea usar firmas digitales.

Los servicios de no repudio deben utilizase cuando se necesita resolver conflictos sobre la ocurrencia o no ocurrencia de un acontecimiento o acción - un conflicto que implica el uso de una firma digital en un contrato

o un pago electrónico -, incluso, pueden ayudar a establecer evidencia para verificar si ha ocurrido un acontecimiento o una acción particular, por ejemplo, la denegación del envío de una instrucción digital firmada usando el correo electrónico. Estos servicios se basan en el uso del cifrado y de las técnicas digitales de firma.

Administración de claves

La administración de claves criptográficas es esencial para el uso eficaz de técnicas criptográficas. Cualquier compromiso o pérdida de claves criptográficas puede comprometer la confidencialidad, autenticidad y/o integridad de la información. Un sistema de administración de la información debe existir para apoyar a la organización en el uso de los dos tipos de técnicas de criptografía, que son:

1. Técnicas de clave secreta, donde dos o más entidades comparten la misma clave y esta clave se utiliza para cifrar y descifrar información. Esta clave tiene que mantenerse en secreto ya que cualquier persona que tiene acceso a ella puede descifrar toda la información cifrada con esa clave, o introducir información no autorizada.

2. Técnicas de clave pública, donde cada usuario tiene un par de claves, una clave pública (se pueda revelar a cualquier persona) y una clave privada (tiene que estar guardada en secreto). Las técnicas de clave pública pueden utilizarse para el cifrado y para producir firmas digitales.

Todas las claves deben protegerse contra la modificación y la destrucción, las claves secretas y privadas necesitan protección contra la divulgación no autorizada, las técnicas criptográficas también se pueden utilizar para este propósito. La protección física debe emplearse para proteger el equipo que genera, almacena y archiva claves.

Un sistema de administración de claves debe basarse en un conjunto de estándares, procedimientos y métodos seguros para:

1. Generar claves mediante diversos sistemas criptográficos y diversas aplicaciones.

2. Generar y obtener certificados de clave pública.

3. Distribuir claves a los usuarios previstos, incluyendo cómo las claves deben activarse cuando se reciban.

4. Almacenar claves, incluyendo cómo los usuarios autorizados obtienen el acceso a éstas.

5. Cambiar o actualizar las claves incluyendo las reglas de cuándo las claves deben cambiarse y cómo se hace esto.

6. Ocuparse de las claves comprometidas.

7. Revocar claves incluyendo cómo las claves deben retirarse o desactivarse, por ejemplo, cuando se han comprometido las claves o cuando un usuario deja una organización (en cuyo caso, las claves también deben archivarse).

8. Recuperar las claves que se pierden o se corrompen como parte de la administración de continuidad del negocio - para recuperar la información cifrada.

9. Archivar claves para la información archivada o respaldada.

10. Destruir claves.

11. Registro y revisión de la administración de claves y las actividades relacionadas.

Para reducir la probabilidad del compromiso, a las claves se les debe definir su fecha de activación y desactivación para que puedan utilizarse solamente por un período de tiempo limitado. Este período de tiempo depende de las circunstancias bajo las cuales se utiliza el control criptográfico y el riesgo percibido.

Algunos procedimientos pueden necesitarse para manejar peticiones legales para el acceso a las claves criptográficas, por ejemplo, la información cifrada puede estar disponible en forma no cifrada como evidencia en un proceso legal, además, debe considerarse el manejo seguro de las claves secretas y privadas y la protección de claves públicas. Existe la amenaza de que alguien que crea una firma digital sustituya una clave pública de algún usuario por la propia, este problema se trata

mediante el uso de un certificado de clave pública, estos certificados se producen de tal manera que atan únicamente la información relacionada con el dueño del par de claves pública y privada a la clave pública. Es por lo tanto importante que el proceso de administración que genera estos certificados sea confiable, por esto, dicho proceso lo realiza normalmente una autoridad de certificación – se trata de una organización reconocida con controles y procedimientos convenientes para proporcionar el grado requerido de confianza.

El contenido de los acuerdos o de los contratos con los proveedores externos de servicios criptográficos - una autoridad de certificación -, debe cubrir aspectos de responsabilidad, confiabilidad de servicios y tiempos de reacción para la disposición de servicios.

d) **Integridad del sistema:** debe proporcionarse un control para la implementación del software en sistemas operacionales. Para reducir al mínimo el riesgo de corrupción de sistemas operacionales, es esencial considerar los controles siguientes:

1. La actualización de las bibliotecas de programas operacionales se debe realizar solamente por el bibliotecario nombrado con la autorización apropiada de la administración.

2. Si es posible, los sistemas operacionales deben contener solamente código ejecutable.

3. El código ejecutable no se debe implementar en un sistema operacional hasta que existan pruebas exitosas y se obtenga la aceptación del usuario, y se hayan actualizado las bibliotecas fuente correspondientes del programa.

4. Mantener un registro de actualizaciones de las bibliotecas de programas operacionales.

5. Versiones anteriores del software se deben conservar como medida de contingencia.

Cualquier decisión para actualizar a una nueva versión del software con un nuevo lanzamiento debe considerar la seguridad del lanzamiento, es decir, la introducción de nueva funcionalidad de seguridad o el número

y severidad de los problemas de seguridad que afectan esta versión. Deben aplicarse parches del software cuando pueden ayudar a quitar o a reducir debilidades de la seguridad. Debe darse acceso físico o lógico solamente a los proveedores para propósitos de soporte cuando es necesario, y con la aprobación de la administración, siempre debe supervisarse las actividades del proveedor.

Es indispensable que los datos de prueba se protejan y controlen, la prueba del sistema y la aceptación requieren generalmente volúmenes substanciales de datos de prueba que estén tan cerca como sea posible a los datos operacionales. Debe evitarse el uso de las bases de datos operacionales que contienen información personal, si tal información se utiliza, debe personalizarse antes de su uso. Los controles siguientes deben aplicarse para proteger los datos operacionales, cuando sean utilizados para propósitos de prueba:

1. Los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacional también deben aplicarse a los sistemas de aplicación de prueba.

2. Debe existir autorización separada cada vez que la información operacional se copia a un sistema de aplicación de prueba.

3. La información operacional se debe borrar de un sistema de aplicación de prueba inmediatamente después de terminar la prueba.

4. El copiado y el uso de la información operacional se deben registrar para tener un registro.

Para reducir el potencial de corrupción en los programas de computadora; debe mantenerse un control estricto sobre el acceso a las bibliotecas fuente del programa como sigue:

1. En lo posible, las bibliotecas fuente del programa no se deben guardar en sistemas operacionales.

2. Debe nombrarse un bibliotecario del programa para cada uso.

3. El personal de soporte de TI no debe tener acceso sin restricción a las bibliotecas fuente del programa.

4. Los programas bajo desarrollo o mantenimiento no deben guardarse en bibliotecas fuente operacionales del programa.

5. La actualización de las bibliotecas fuente del programa y la emisión de las fuentes del programa a los programadores, deben realizarse solamente por el bibliotecario nombrado y autorizado por el encargado de TI para la aplicación.

6. Los listados del programa deben mantenerse en un ambiente seguro.

7. Debe mantenerse un registro de todos los accesos a las bibliotecas fuente del programa.

8. Las viejas versiones de los programas fuente deben archivarse, con una indicación clara de las fechas y de los tiempos exactos en que eran operacionales, junto con todo el software de soporte, control de trabajo, definiciones de los datos y procedimientos.

9. El mantenimiento y el copiado de las bibliotecas fuente del programa deben estar conforme a procedimientos estrictos del control del cambio.

e) Seguridad en el desarrollo:

Procedimientos del control de cambios

Para reducir al mínimo la corrupción de los sistemas de información, debe existir un control estricto de la implementación de cambios. Los procedimientos formales del control del cambio deben hacerse cumplir, para asegurarse de que los procedimientos de seguridad y de control no se comprometan, que a los programadores de apoyo se les dé el acceso solamente a esas partes del sistema necesarias para su trabajo, y que se obtenga el acuerdo y la aprobación formales para cualquier cambio. Al cambiar el software de aplicación se puede afectar el ambiente operacional, por esto, dondequiera que se aplique, deben integrarse los procedimientos operacionales del control del cambio. Este proceso debe:

1. Mantener un registro de los niveles de autorización convenidos.

2. Asegurar que los cambios los realicen usuarios autorizados.

3. Revisar controles y procedimientos de integridad para asegurar que no se comprometen debido a los cambios.

4. Identificar todo el software de la computadora, información, entidades de la base de datos y hardware que requieren modificación.

5. Obtener la aprobación formal de las ofertas detalladas antes de comenzar el trabajo.

6. Asegurar que el usuario autorizado acepte cambios antes de cualquier implementación.

7. Asegurar que la puesta en práctica se realice para reducir al mínimo la interrupción del negocio.

8. Asegurar que la documentación del sistema se actualice al completarse cada cambio y de que la vieja documentación se archive.

9. Mantener un control de la versión para todas las actualizaciones del software.

10. Mantener un registro de todas las peticiones de cambio.

11. Asegurar que la documentación de operación y los procedimientos del usuario se cambien de manera necesaria para ser apropiados.

12. Asegurar que la implementación de los cambios ocurra en el tiempo correcto y no interfiera con los procesos del negocio implicados.

En muchas organizaciones existe un ambiente en el cual los usuarios prueban el nuevo software y a su vez éste se encuentre separado de los ambientes de desarrollo y de producción, esto permite tener control sobre el nuevo software y protección adicional de la información operacional que se utiliza para propósitos de prueba.

Cambios al sistema operativo y a los paquetes de software

Es necesario cambiar el sistema operativo periódicamente, por ejemplo, para instalar una nueva versión, actualización o parches. Cuando ocurren los cambios, se deben revisar y probar los sistemas de aplicación para

asegurar que no hay impacto adverso en la operación o la seguridad. Este proceso debe cubrir:

1. Revisión del control de aplicación y los procedimientos de integridad para asegurar que no se comprometieron debido a los cambios en el sistema operativo.

2. Asegurar que el plan y el presupuesto anuales de apoyo cubran las revisiones y las pruebas del sistema debido a los cambios en el sistema operativo.

3. Asegurar que la notificación de los cambios en el sistema operativo se proporcione a tiempo para permitir que las revisiones ocurran antes de la implementación.

4. Asegurar que se realicen los cambios apropiados a los planes de continuidad del negocio.

Deben desaprobarse modificaciones a los paquetes de software, los paquetes de software provistos por el vendedor deben utilizarse sin modificación, cuando es esencial modificar un paquete de software, los puntos siguientes deben tomarse en cuenta:

1. Si puede obtenerse el consentimiento del vendedor.

2. La posibilidad de obtener los cambios como actualizaciones estándares del programa.

3. El impacto como resultado de los cambios si la organización llega a ser responsable del mantenimiento futuro del software.

Si los cambios se vuelven esenciales, el software original debe conservarse y los cambios deben aplicarse a una copia claramente identificada. Todos los cambios deben probarse completamente y documentarse para poderse aplicar a futuras actualizaciones del software.

Canales secretos y código de Troya

Un canal secreto puede exponer la información a través de medios indirectos. Puede activarse cambiando un parámetro accesible mediante

elementos seguros e inseguros de un sistema de cómputo, o incluyendo la información en una secuencia de datos. El código de Troya se diseña para afectar un sistema de una manera no autorizada. Los canales secretos y el código de Troya ocurren raramente por accidente, cuando los canales secretos o el código de Troya son una preocupación latente, se debe considerar lo siguiente:

1. Comprarle programas solamente a una fuente respetable.

2. Comprar programas en código fuente de tal manera que el código pueda verificarse.

3. Utilizar productos evaluados.

4. Inspeccionar todo el código fuente antes de su uso operacional.

5. Controlar el acceso y la modificación al código una vez instalado.

6. Utilizar personal de confianza para trabajar en sistemas claves.

Desarrollo de software por una organización externa

Cuando el desarrollo de software lo realiza una organización externa, es conveniente considerar los puntos siguientes:

1. Autorización de arreglos, propiedad del código y derechos de propiedad intelectual.

2. Certificación de la calidad y de la exactitud del trabajo realizado.

3. Mantener en un documento cerrado y sellado las acciones/acuerdos en caso de que falle la tercera entidad.

4. Derechos de acceso para verificar la calidad y la exactitud de los trabajos hechos.

5. Requerimientos contractuales de la calidad del código.

6. Prueba antes de la instalación para detectar el código de Troya.

APÉNDICE I

PLAN DE CONTINUIDAD DEL NEGOCIO

a) Planeamiento de la continuidad del negocio:

Proceso de la administración de la continuidad del negocio

Debe existir un proceso para desarrollar y mantener continuidad del negocio en toda la organización, es conveniente que reúna los elementos dominantes siguientes de la administración de la continuidad del negocio:

1. Entender los riesgos que la organización enfrenta en términos de su probabilidad y de su impacto, incluyendo una identificación y prioridad de los procesos críticos del negocio.

2. Entender el impacto que las interrupciones pueden tener en el negocio (es importante encontrar soluciones para manejar incidentes más pequeños, así como los incidentes serios que podrían amenazar la viabilidad de la organización) y establecer los objetivos de negocio de los medios de procesamiento de la información.

3. Considerar la compra de un seguro conveniente que puede formar parte del proceso de continuidad del negocio.

4. Formular y documentar una estrategia de continuidad del negocio constante con los objetivos y las prioridades de negocio.

5. Formular y documentar los planes de continuidad del negocio de acuerdo con la estrategia convenida.

6. Pruebas y actualizaciones regulares de los planes y de los procesos puestos existentes.

7. Asegurar que la administración de la continuidad del negocio esté incorporada en los procesos y estructura de la organización. La responsabilidad para coordinar el proceso de administración de la continuidad del negocio debe colocarse en un nivel apropiado dentro de la organización, por ejemplo, en el foro de seguridad de la información.

La continuidad del negocio debe comenzar con la identificación de los acontecimientos que pueden causar interrupciones a los procesos del negocio, por ejemplo, inundación, falla del equipo y fuego, esto debe

realizarse mediante una evaluación de riesgo para determinar el impacto de esas interrupciones (ambos en términos de la escala de daños y del período de recuperación). Es indispensable que tales actividades se realicen con la participación completa de los dueños de los recursos y de los procesos del negocio. La evaluación considera todos los procesos del negocio, y no se limita a las instalaciones de procesamiento de la información, dependiendo de los resultados de la evaluación de riesgo, debe desarrollarse un plan de estrategia para lograr la continuidad del negocio. Una vez que se haya creado este plan, debe ser distribuido por la administración.

Escritura e implementación de los planes de continuidad

Es necesario desarrollar planes para mantener o restaurar los procesos críticos del negocio en un cierto período de tiempo después de la interrupción o falla. El proceso de planeamiento de la continuidad del negocio debe considerar lo siguiente:

1. Identificación y acuerdo de todas las responsabilidades y procedimientos de emergencia.

2. Implementación de los procedimientos de emergencia para permitir la recuperación y la restauración en períodos de tiempo requeridos. Prestar atención en la evaluación de las dependencias externas del negocio y de los contratos existentes.

3. Documentación de procedimientos y de procesos convenidos.

4. Capacitación apropiada del personal en los procedimientos y los procesos de emergencia, incluyendo la administración de la crisis.

5. Prueba y actualización de los planes.

El proceso de planeamiento debe enfocarse en los objetivos de negocio - por ejemplo, restauración de servicios específicos a los clientes en un período de tiempo aceptable -, los servicios y los recursos, incluyendo el suministro de personal y procesamiento de recursos.

Debe mantenerse un solo marco de los planes de continuidad del negocio para asegurar que todos los planes son constantes y para

identificar las prioridades de prueba y mantenimiento, cada plan de la continuidad del negocio debe especificar claramente las condiciones para su activación, así como los individuos responsables para ejecutar cada componente del plan. Cuando se identifican los nuevos requerimientos, los procedimientos de emergencia establecidos - por ejemplo, planes de evacuación o cualquier arreglo existente de retroceso - deben modificarse de forma apropiada. Un marco para el planeamiento de la continuidad del negocio debe considerar lo siguiente:

1. Las condiciones para activar los planes que describen el proceso que se seguirá (cómo determinar la situación, quién está implicado, etc.) antes de que se active cada plan.

2. Los procedimientos de emergencia que describen las acciones que se tomarán después de un incidente que comprometa operaciones de negocio y/o vidas humanas. Esto debe incluir acciones para realizar la administración de las relaciones públicas y mantener el contacto con las autoridades públicas apropiadas - policía, bomberos y gobierno local.

3. Procedimientos de reanudación que describen las acciones para mover actividades económicas o servicios de apoyo a lugares alternativos temporales, y reanudar procesos de negocio en un período de tiempo requerido.

4. Procedimientos de reanudación que describen las acciones que se llevarán a cabo para regresar a las operaciones normales de negocio.

5. Un horario de mantenimiento que especifica cómo y cuándo el plan se probará y cuál es el proceso para mantener el plan.

6. Actividades de prevención y capacitación que se diseñan para lograr la comprensión de los procesos de continuidad del negocio y para asegurar que los procesos continúan siendo eficaces.

7. Las responsabilidades de los individuos, describiendo quién es responsable para ejecutar cierto componente del plan. Las alternativas deben nombrarse según se requiera.

Cada plan debe tener un dueño específico. Los procedimientos de emergencia y los planes de reanudación deben ser responsabilidad de los dueños de los recursos o de los procesos implicados del negocio. Las acciones de reanudación para los servicios técnicos alternativos, tales como tratamiento de la información e instalaciones de comunicación, deben ser responsabilidad de los proveedores de servicio.

b) **Prueba de la continuidad del negocio:** existen técnicas que pueden utilizarse para proporcionar la seguridad de que el plan funcionará verdaderamente:

1. Prueba de varios escenarios (que discuten las acciones para la recuperación del negocio usando interrupciones de ejemplo).

2. Simulaciones (particularmente para entrenar a la gente en sus papeles de administración de crisis después de los incidentes).

3. Prueba técnica de recuperación (asegurar que los sistemas de información se pueden restaurar con eficacia).

4. Prueba de recuperación en un sitio alterno (procesos de funcionamiento del negocio en paralelo con operaciones de recuperación lejos del sitio principal).

5. Pruebas de las instalaciones y de los servicios del proveedor (asegurar que los servicios externamente proporcionados y los productos resolverán el compromiso contraído).

6. Ensayos completos (que prueban que la organización, el personal, las instalaciones del equipo y los procesos pueden hacer frente a interrupciones).

Las técnicas se pueden utilizar por cualquier organización y deben reflejar la naturaleza del plan de recuperación específico.

c) **Mantenimiento de la continuidad del negocio:** ejemplos de situaciones que pueden hacer necesaria la actualización de los planes incluyen la adquisición de equipo nuevo, o la actualización de sistemas y cambios operacionales en:

1. Personal.
2. Direcciones o números de teléfono.
3. Estrategia de negocio.
4. Lugares, instalaciones y recursos.
5. Legislación.
6. Contratistas, proveedores y clientes clave.
7. Procesos nuevos o removidos.
8. Riesgo (operacional y financiero).

APÉNDICE J

CUMPLIMIENTO

a) **Requerimientos legales:** el diseño, la operación, el uso y la administración de los sistemas de información pueden estar conforme a requerimientos estatutarios, reguladores y contractuales de seguridad, es conveniente buscar consejos sobre requerimientos legales específicos en los asesores jurídicos de la organización, o en los practicantes legales calificados, los requerimientos legislativos varían de país a país y para la información creada en un país que se transmite a otro (es decir, flujo de datos transmitidos). Los requerimientos relevantes de tipo estatutarios, reguladores y contractuales se deben definir y documentar explícitamente para cada sistema de información. Los controles y las responsabilidades individuales para alcanzar estos requerimientos deben definirse y documentarse de manera semejante.

Derechos de propiedad intelectual

Deben implementarse los procedimientos apropiados para usar material con restricciones legales a los derechos de propiedad intelectual, tales como el derecho de copia, derechos de diseño, marcas comerciales. La infracción en los derechos de copia puede conducir a una demanda legal que puede implicar procedimientos criminales. Los requerimientos legislativos, reguladores y contractuales restringen el copiado del material, lo cual indica que sólo podrá utilizarse el material que sea desarrollado por la organización, o que sea permitido o proporcionado por el desarrollador de la organización.

Los productos propietarios de software se proveen generalmente según los términos de la licencia que limita el uso de los productos en máquinas específicas y puede limitar su copiado a la creación de copias de respaldo solamente. Deben considerarse los controles siguientes:

1. Publicar una política de cumplimiento de los derechos de copia del software que define el uso legal del software y de los productos de información.

2. Manejar estándares para los procedimientos de adquisición de productos de software.

3. Mantener conocimiento de las políticas de derecho de copia y de adquisición del software, y dar aviso de la acción disciplinaria tomada en contra del personal que las viole.

4. Mantener registros apropiados del activo.

5. Mantener prueba y evidencia de la propiedad de licencias, de discos principales, de manuales, etc.

6. Implementar controles para asegurar que no se excede ningún número máximo de usuarios permitidos.

7. Realizar la verificación de que solamente el software autorizado y los productos con licencia estén instalados.

8. Proporcionar una política para mantener las condiciones de licencia apropiadas.

9. Proveer una política para transferir o disponer del software de otros.

10. Usar herramientas apropiadas de verificación.

11. Cumplir con términos y condiciones para el software y la información que se obtienen de redes públicas.

Resguardo de los registros de la organización

Los registros importantes de una organización deben protegerse contra pérdida, destrucción y falsificación, es posible que algunos registros necesiten conservarse con seguridad para mantener los requerimientos estatutarios o reguladores, así como para apoyar actividades esenciales del negocio. Ejemplos de esto son los registros que pueden requerirse como evidencia de que una organización funciona dentro de reglas estatutarias o reguladoras, o para asegurar la defensa adecuada contra la acción civil o criminal potencial, o confirmar el estado financiero de una organización con respecto a accionistas, a socios y a auditores. El período de tiempo y el contenido de los datos para la retención de información se puede fijar mediante una ley o regulación nacional. Es importante que los registros se clasifiquen en diferentes tipos - registros estadísticos, registros de base de datos, registros de transacción, registros de verificación y procedimientos operacionales - cada uno con detalles de períodos de validez y tipo de medios de almacenamiento - papel, microficha, magnético, óptico. Cualquier clave criptográfica relacionada a archivos cifrados o a firmas digitales, debe guardarse con seguridad y ponerse a disposición de las

personas autorizadas cuando se necesite. No es conveniente descartar la posibilidad de degradación de los medios usados para el almacenamiento de los registros. Por lo que deben implementarse procedimientos de almacenamiento y manejo con base en las recomendaciones del fabricante. Cuando se eligen medios de almacenamiento electrónicos, los procedimientos para asegurar la capacidad de acceso a los datos (los medios y legibilidad del formato) a través de un período de validez, deben incluirse para salvaguardarlos contra la pérdida debido al cambio futuro de la tecnología. Los sistemas de almacenamiento de datos deben elegirse de tal forma que los datos requeridos se puedan presentar de una manera aceptable en una corte en caso de que se necesite presentarlos como evidencia. El sistema de almacenamiento y de manejo debe asegurar la identificación clara de registros y su período de validez estatutario o regulador, por lo que es indispensable permitir la destrucción apropiada de los registros después de ese período si ya no los necesita la organización. Para cubrir estas obligaciones, se deben tomar las medidas siguientes dentro de una organización:

1. Se deben publicar y seguir las pautas para el almacenamiento, dirección y disposición de registros y de información.

2. Debe elaborarse un horario de retención, identificando tipos de registro esenciales y el período de tiempo durante el cual deben conservarse.

3. Debe mantenerse un inventario de fuentes de información clave.

4. Se deben implementar controles apropiados para proteger registros e información esenciales contra pérdida, destrucción y falsificación.

Protección de los datos y aislamiento de la información personal

Algunos países han introducido la legislación colocando controles en el procesamiento y transmisión de los datos personales, tales controles pueden imponer obligaciones en el procesamiento y diseminado de la información personal, y pueden restringir la capacidad para transferir esos datos a otros países. El cumplimiento con la legislación de protección de datos requiere una administración de la estructura y el control apropiados, esto se logra a menudo mediante la visita de un oficial de protección de datos que guía a los administradores, usuarios y proveedores de servicio en sus responsabilidades individuales y los procedimientos específicos que

deben seguirse. Debe ser responsabilidad del dueño de la información, informar al oficial de protección de datos sobre cualquier propuesta para mantener la información personal en un archivo estructurado y para asegurar el conocimiento de los principios de protección de datos definidos por la legislación correspondiente.

Prevención del mal uso de las instalaciones de procesamiento de la información

Las instalaciones o medios de procesamiento de la información de una organización se proporcionan para propósitos del negocio, por lo que, la administración debe autorizar su uso. Cualquier uso de estas instalaciones o medios no específico del negocio o para propósitos no autorizados, sin la aprobación de la administración, se debe considerar como uso incorrecto de las instalaciones o medios. Si tal actividad se identifica mediante medios de supervisión u otros, debe atraer la atención del administrador individual que se nombra para tal acción disciplinaria. La legalidad para supervisar el uso varía de país a país y puede requerir que los empleados sean aconsejados para tal supervisión. El asesoramiento jurídico debe realizarse antes de implementar los procedimientos de supervisión, muchos países tienen, o están en proceso de introducir la legislación para protegerse contra el mal uso de la computadora, ya que puede ser una actividad criminal utilizar una computadora para propósitos no autorizados, es por lo tanto esencial que todos los usuarios se enteren del alcance exacto de su acceso permitido. Para lograr lo anterior, es conveniente dar a los usuarios una autorización escrita, una copia que debe firmar el usuario y que la organización debe conservar con seguridad. Los empleados de una organización, y los usuarios externos, deben enterarse de que no se permite ningún acceso excepto ése al que están autorizados, por lo tanto, cuando se realice una conexión, un mensaje de alerta debe presentarse en la pantalla de la computadora para indicar que el sistema al que se está entrado es privado y que el acceso no autorizado no se permite. El usuario tiene que reconocer y reaccionar apropiadamente al mensaje en la pantalla para continuar con el proceso de conexión.

Regulación de controles criptográficos

Algunos países han implementado acuerdos, leyes, regulaciones u otros instrumentos para controlar el acceso o el uso de controles criptográficos. Tal control puede incluir:

1. Importación y/o exportación del hardware y del software para realizar funciones criptográficas.

2. Importación y/o exportación del hardware y del software que se diseña para tener funciones criptográficas agregadas a ellos.

3. Métodos obligatorios o discrecionales de los países para el acceso a la información cifrada por hardware o el software para proporcionar la confidencialidad del contenido.

Debe solicitarse el asesoramiento jurídico para asegurar el cumplimiento con la ley nacional, se debe tener asesoramiento jurídico antes de que la información cifrada o los controles criptográficos se vayan a otro país.

Recolección de evidencia

Es necesario contar con la evidencia adecuada para apoyar acciones contra una persona o una organización, siempre que esta acción sea una cuestión disciplinaria interna, la evidencia necesaria se describirá mediante procedimientos internos. Cuando la acción implique la ley civil o criminal, la evidencia que se presente debe cumplir con reglas planteadas en la ley relevante o en las reglas de la corte específica en la cual el caso se presenta. En general, estas reglas cubren:

1. Admisibilidad de la evidencia: si la evidencia se puede o no utilizar en la corte.

2. Peso de la evidencia: la calidad y lo completo que está la evidencia.

3. Evidencia adecuada de que los controles han funcionado correctamente y constantemente (es decir evidencia del control de proceso) durante el período en que la evidencia que se recupera fue almacenada y procesada por el sistema.

Para alcanzar la admisibilidad de la evidencia, las organizaciones deben asegurar que sus sistemas de información cumplan con cualquier estándar o código de práctica publicado para la producción de evidencia admisible. Para alcanzar la calidad y lo completo de la evidencia, un

indicio fuerte de evidencia es necesario. En general, un rastro tan fuerte se puede establecer bajo las condiciones siguientes:

1. Para los documentos en papel: el original se guarda con seguridad y se registra quién lo encontró, donde fue encontrado, cuándo fue encontrado y quién atestiguó el descubrimiento.

2. Para la información en medios de cómputo: se deben realizar copias en cualquier medio removible, información en discos duros o en memoria para asegurar su disponibilidad. Debe guardarse el registro de todas las acciones durante el proceso de copiado y atestiguarse el proceso. Una copia de los medios y del registro debe guardarse con seguridad.

Cuando un incidente se detecta, puede no ser obvio que dará lugar a una acción legal, por lo tanto, el peligro existe de que la evidencia necesaria se destruya accidentalmente antes de que se observe la seriedad del incidente. Es recomendable implicar a un abogado o a un policía en cualquier demanda legal contemplada y ser aconsejado sobre la evidencia requerida.

b) **Requerimientos técnicos:** los administradores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, además, a todas las áreas dentro de la organización se les debe realizar una revisión regular para asegurar su cumplimiento con políticas y estándares de seguridad. Éstas deben incluir lo siguiente:

1. Sistemas de información.

2. Proveedores de sistemas.

3. Dueños de la información y de los activos de información.

4. Usuarios.

5. Administración.

Es importante que los dueños de los sistemas de información apoyen las revisiones regulares del cumplimiento de sus sistemas con las políticas

apropiadas de seguridad, los estándares y cualquier otro requisito de seguridad.

Los sistemas de información se deben verificar regularmente para saber si cumplen con estándares de implementación de seguridad. La verificación del cumplimiento técnico implica la inspección de los sistemas operacionales para asegurarse de que los controles de hardware y de software se hayan implementado correctamente. Este tipo de comprobación del cumplimiento requiere asistencia técnica especializada, ésta debe realizarse manualmente (apoyada en herramientas apropiadas de software, en caso de ser necesario) por un ingeniero experimentado del sistema, o por un paquete de software automatizado que genere un informe técnico para interpretarse posteriormente por un especialista técnico. El cumplimiento cubre, por ejemplo, la prueba de penetración, que se puede realizar mediante expertos independientes específicamente contratados para este propósito. Este punto puede ser útil para la detección de vulnerabilidades en el sistema y para comprobar qué tan eficaces son los controles que previenen el acceso no autorizado debido a estas vulnerabilidades. Es conveniente tomar las medidas necesarias en caso de que una prueba de penetración conduzca a un compromiso de la seguridad del sistema y explote inadvertidamente otras vulnerabilidades. Cualquier verificación del cumplimiento técnico se debe realizar solamente por, o bajo supervisión de, las personas autorizadas competentes.

b) **Revisiones del sistema:** los requerimientos de revisión y las actividades que implican verificación en los sistemas operacionales deben planearse cuidadosamente y acordarse para reducir al mínimo el riesgo de interrupciones a los procesos del negocio. Lo que sigue debe observarse:

1. Los requisitos de verificación deben convenirse con la administración apropiada.

2. Debe convenirse y controlarse el alcance de las verificaciones.

3. Las verificaciones deben limitarse al acceso de sólo lectura de software y de los datos.

4. El acceso que no sea de sólo lectura debe permitirse solamente en copias aisladas de los archivos del sistema y que se borran cuando se termina la revisión.

5. Deben identificarse explícitamente y hacerse disponibles los recursos de TI para realizar verificaciones.

6. Deben identificarse y convenirse los requerimientos para el proceso especial o adicional.

7. Todo el acceso debe supervisarse y registrarse para producir indicios de referencia.

8. Deben documentarse todos los procedimientos, requerimientos y responsabilidades.

Debe protegerse el acceso a las herramientas de verificación del sistema, es decir, software o archivo de datos, para prevenir cualquier mal uso o compromiso posible, estas herramientas deben separarse del desarrollo y sistemas operacionales y no guardarse en bibliotecas de cintas o áreas de usuario, a menos que se les dé un nivel apropiado de protección adicional.

APÉNDICE K

GLOSARIO DE TÉRMINOS

Aceptación del riesgo: decisión para aceptar un riesgo.

Activo: es todo aquello con valor para una organización y que necesita protección - datos, infraestructura, hardware, software, personal y su experiencia, información, servicios.

ALE: Annual Loss Expectancy - Expectativa de Pérdida Anual.

Amenaza: es una fuerza potencial que puede degradar la confidencialidad, integridad o disponibilidad de un sistema o red. Las amenazas pueden ser humanas (intencionales o no intencionales) o ambientales (naturales o fabricadas).

Análisis de riesgo: evaluación de amenazas y vulnerabilidades de la información y su impacto en el procesamiento de la información así como su probabilidad de ocurrencia.

Análisis del riesgo de seguridad: es una inspección de las interrelaciones entre activos, amenazas, vulnerabilidades y contramedidas para determinar el actual nivel de riesgo.

BCS: British Computer Society - Sociedad Británica de Cómputo.

BS: British Standard – Estándar Británico.

BS7799: es el estándar británico para el manejo de la seguridad informática.

BSI: British Standard Institute - Instituto Británico de Estándares.

CCSC: Commercial Computer Security Centre - Centro Comercial de Seguridad en Cómputo.

CCTA: Central Computer and Telecommunications Agency - Agencia Central de Cómputo y Telecomunicaciones.

COBRA: Consultative, Objective and Bi-functional Risk Analysis - Análisis Consultivo, Objetivo y Bifuncional del Riesgo.

Conceptual: Perteneciente o relativo al pensamiento expresado con palabras después de examinadas las circunstancias.

Controles: son los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización. Medida contra vulnerabilidades. Presentan una meta que debe ser alcanzada y lo que debe hacerse – puntos que deben ponerse en práctica - para lograrla.

CSRC: Computer Security Resource Center - Centro de recursos de seguridad en cómputo.

DISC: Delivering Information Solutions to Customers - Departamento de Entrega de Soluciones de Información para Clientes.

DSL: Digital Subscriber Line – Línea digital de suscriptor. Una tecnología que permite a los datos, voz y video mezclarse y llevarse sobre líneas telefónicas analógicas estándar. Esto se logra utilizando las frecuencias que no se usan y están disponibles en una línea telefónica.

DTI: British Department of Trade and Industry - Departamento Británico de Comercio e Industria.

EAC: Estimated Annual Cost - Costo Anual Estimado.

EAL: Equipment Assurance Level - Nivel de Garantía del Equipo.

EDI: Electronic Data Interchange – Intercambio Electrónico de Datos.

Estatutario: Conforme a las disposiciones o reglas legales.

Evaluación del riesgo: comparación de los resultados de un análisis del riesgo con los criterios estándares del riesgo u otros criterios de decisión.

Fiabilidad: Probabilidad del buen funcionamiento de una cosa.

GASSP: Generally Accepted System Security Principles - Principios Generalmente Aceptados de Seguridad del Sistema.

GMITS: Guidelines for the Management of IT Security - Principios para el Manejo de Seguridad de Tecnología de Información.

IEC: International Electrotechnical Comission - Comisión Internacional Electrotécnica.

Impacto: pérdidas como resultado de la actividad de una amenaza.

IRCA: International Register of Certified Auditors - Registro Internacional de Auditores Certificados.

ISDN: Integrated Services Digital Network – Red Digital de Servicios Integrados. Un servicio portador que las compañías de teléfonos ofrecen y está diseñada para transmitir comunicaciones de voz y no voz (por ejemplo, fax, video, datos de computadoras) sobre la misma red.

ISMS: Information Security Management System - Sistema de Administración de Seguridad de la Información (SASI). ISMS es el medio por el cual se supervisa y controla la seguridad, minimizando el riesgo residual del negocio y asegurando que la seguridad continúa cumpliendo con los requerimientos corporativos, legales y del cliente.

ISO: International Organization for Standardization - Organización Internacional para la Estandarización.

IT: Information Technology. Véase TI.

ITSEC: Information Technology Security Evaluation Criteria - Criterios de Evaluación de Seguridad de Tecnología de la Información.

Manejo del riesgo: proceso de identificación, control y minimización o eliminación de riesgos de seguridad que pueden afectar sistemas de información, por un costo aceptable.

NCC: National Computing Centre - Centro Nacional de Cómputo.

NIST: National Institute of Standards and Technology – Instituto Nacional de Estándares y Tecnología.

OECD: Organisation for Economic Co-operation and Development – Organización para la Cooperación Económica y el Desarrollo.

Pérdida esperada: el impacto anticipado y negativo a los activos debido a una manifestación de la amenaza.

Perpetrador: es aquel individuo que se basa en cualquier medio para ejecutar o consumar un delito o culpa grave.

Potencial: Que puede suceder o existir, pero no existe aún.

Riesgo: posibilidad de sufrir algún daño o pérdida.

Riesgo residual: El nivel de riesgo que queda después de la consideración de todas las medidas necesarias, los niveles de vulnerabilidad y las amenazas relacionadas. Éste debe ser aceptado como es o reducirse a un punto donde pueda ser aceptado.

SANS: SysAdmin, Audit, Network, Security – Administración de sistemas, auditoría, red, seguridad.

SASI: Information Security Management System (ISMS) - Sistema de Administración de Seguridad de la Información. SASI es el medio por el cual se supervisa y controla la seguridad, minimizando el riesgo residual del negocio y asegurando que la seguridad continúa cumpliendo con los requerimientos corporativos, legales y del cliente.

SEDISI: Asociación Española de Empresas de Tecnologías de la Información.

Seguridad de la información: se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información, con ello se obtiene confianza en que la información está debidamente resguardada y que no hay peligro que temer.

TI: La tecnología de la información es un término que comprende todas las formas de tecnología empleadas para crear, almacenar, intercambiar y usar información en sus formas variadas (datos de negocios, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquéllas que aún no se han concebido.) Es un término conveniente para incluir tanto a la telefonía como a la tecnología de cómputo en una misma palabra.

UCT: Universal Co-ordinated Time – Tiempo Coordinado Universal.

UKAS: the United Kingdom Accreditation Service - Servicio de Acreditación del Reino Unido.

UPS: Uninterruptable Power Supply – Fuente de Alimentación Ininterrumpible.

Vulnerabilidad: es una condición de debilidad la cual puede ser explotada por una o más amenazas.

VPN: Vitual Private Network – Red Privada Virtual.

BIBLIOGRAFÍA

1. A framework for measuring and implementing information security philby.ucsd.edu/~cse291_IDVA/papers/ rating-position/Martins.pdf

2. An overview of BS7799 http://www.dunelmsystems.co.uk/bs7799.html#1

3. Bhaskar, K. *Computer security. Threats and countermeasures*. England, NCC Blackwell, 1993.

4. British Standard 7799 (ISO 17799) http://www.knowledgeleader.com/iafreewebsite.nsf/content/SecurityBritish Standard7799ISO17799?OpenDocument

5. BS7799 Compliancy And Certification http://www.webpronews.com/it/itmanagement/wpn-18-20040224BS7799 CompliancyandCertification.html

6. Business information http://www.bsi-global.com

7. Certificación BS7799-2 http://www.hi-end-business-security.com/psg-hebs/HEBS-A30.htm

8. CONET http://www.conet.com.mx/principal.htm

9. Criterios comunes http://www.commoncriteriaportal.org/

10. Definición de información http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212343,00.html

11. E-Security articles http://www.mielesecurity.com/articles.htm

12. Evaluación de la seguridad de un sistema de información http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

13. García-Pelayo, Ramón. *Pequeño Larousse Ilustrado*. México, Ediciones Larousse, 1987.

14. Generally Accepted System Security Principles (GASSP)
http://web.mit.edu/security/www/gassp1.html

15. Gestión de la seguridad
http://www.rediris.es/cert/doc/unixsec/node31.html

16. Global information security survey
http://www.kpmg.com.mx/publicaciones/pdf/global_info.pdf

17. Gutiérrez, Sergio, Quezada, Cintia. *Tesis: Fundamentos de seguridad de la información*. México, Facultad de Ingeniería UNAM, 2001.

18. How 7799 works
http://www.gammassl.co.uk/bs7799/works.html

19. Importancia del Análisis de Riesgo de Seguridad
http://seguridad.internet2.ulsa.mx/congresos/ 2003/cudi2/impariesgo.pdf

20. Incident response requirements under ISO 17799
http://www.guidancesoftware.com/corporate/whitepapers/downloads/ ISO17799.pdf

21. Information security management: understanding ISO 17799
http://www.lucent.com/livelink/209341_Whitepaper.pdf

22. Information security management standard? ISO 17799 / BS7799
http://www.entiretyservices.com/Security%20White%20Paper.pdf

23. Information security management systems
http://www.software.org/security/security_isms.asp

24. Information security management systems and standards
http://www.itsc.org.sg/synthesis/2001/itsc-synthesis2001-thowchang-siewmun-alvinfoo-isms.pdf

25. Information technology
http://whatis.techtarget.com/definition/0,289893,sid9_gci214023,00.html

26. Introduction to security risk analysis
http://www.security-risk-analysis.com/

27.ISO
http://www.iso.ch

28.ISO 17799
http://www.iso-17799.com/buy17799.htm

29.ISO 17799 – Information security management synopsis
http://healthnet.hnet.bc.ca/hds/approved_standards/ ISO17799synopsis.pdf

30.ISO 17799: La nueva norma técnica global de seguridad
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1261.html

31.ISO 17799 Security standard: ISO17799 compliance & positioning
http://www.securityauditor.net/iso17799/how.htm

32.ISO 17799 - The information security standard
http://www.standardsdirect.org/iso17799.htm

33.ISO 17799 - What is ISO 17799 (the ISO security standard)?
http://matrix0.members.beeb.net/iso-17799/index.htm

34.ISO 17799: What is it?
http://www.iso17799software.com/what.htm

35.La norma BS7799 al alcance de su empresa
http://www.symantec.com/region/mx/enterprisesecurity/content/government/LAM_356.html

36.Lista de estándares de seguridad internacionales
http://www.unal.edu.co/seguridad/estandares_de_seguridad_internacionales.pdf

37.Métodos y seguridad de un sistema de información
http://www.ssi.gouv.fr/es/confianza/documents/bs7799-es.html

38.Other disaster recovery related web sites
http://www.disasterrecoveryworld.com/weblinks.htm

39.¿Qué es el BS 7799-2:2002?
http://centrum.pucp.edu.pe/Centro_Excelencia/BS7799-2_2002.htm

40. ¿Qué es el ISO 17799?
http://www.cdd.com.mx/iso17799.asp

41. Resources for security risk analysis, ISO 17799 / BS7799
Security policies & security audit
http://www.securityauditor.net/

42. Risk analysis, assessment, management
http://www.nr.no/~abie/RiskAnalysis.htm

43. Risk Analysis Methodologies
http://home1.pacific.net.sg/~thk/risk.html

44. Roche launches the new UK standard for information security
http://www.newsrelease-archive.net/coi/depts/GTI/coi0855e.ok

45. The RUSecure™ Information Security Policies
http://www.information-security-policies.com/download.htm

46. Security management practices. ISO 17799 is stand for information security management!
http://www.cccure.org/Documents/RyanSebastian/SecurityManagementPractices.pdf

47. Security: Rallying to the standard
http://www.computerweekly.com/Article21458.htm

48. Security risk analysis and management
http://www.cs.kau.se/~albin/Documents/RA_by%20Jenkins.pdf

49. Security web site home page
http://www.software.org/security/security_isms.asp

50. Seguridad de la información: ISO 17799, BS7799, Análisis del riesgo de la seguridad y soluciones de la política de la seguridad
http://www.security.kirion.net/seguridad/

51. Seguridad en informática
http://www.bulltek.com/Spanish_Site/ISO%209000%20INTRODUCCION/TL%209000%20Spanish/ISO_17799_Spanish/iso_17799_spanish.html

52. Seguridad: Índice general
http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node1.html

53. Seguridad: Introducción
http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node332.html

54. Seguridad ISO 17799
http://www.cpci.org.ar/newsletters/91/seguridad.htm

55. Seguridad y control en el ambiente informático
http://www.pwc.com/images/soacat/febreromarzo2003.pdf

56. Seguridad y tecnología de información, algo más que una moda
http://www.chein.com.mx/articulos/2mar-2002.htm

57. Summers, Rita. *Secure Computing, Threats and Safeguards*. E.U.A., Mc Graw Hill, 1997.

58. The ISO 17799 and BS7799 Portal
BS 7799 / ISO 17799 Software & Resources
http://website.lineone.net/~matrix0/iso17799/othersites.htm

59. The ISO 17799 directory
http://www.iso-17799.com/

60. The road to BS7799, accreditation and using ISO 17799 as an information security framework
http://www.itsecurity.com/papers/idefence1.htm

61. Tomando en serio la seguridad de la información
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1333.html

62. What is: ISO17799?
http://www.securityauditor.net/iso17799/what.htm