NORMA TÉCNICA PERUANA

NTP-ISO/IEC 17799 2007

Comisión de Reglamentos Técnicos y Comerciales - INDECOPI
Calle de La Prosa 138, San Borja (Lima 41) Apartado 145 Lima, Perú

EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información

EDI. Information technology. Code of practice for information security management

(EQV. ISO/IEC 17799:2005 Information technology. Code of practice for information security management)

2007-01-16
2ª Edición

R.001-2007/INDECOPI-CRT. Publicada el 2007-01-22 Precio basado en 173 páginas

I.C.S.: 35.040 ESTA NORMA ES RECOMENDABLE

Descriptores: EDI, tecnología de la información, información multimedia e hipermedia, técnicas de seguridad IT, código de barras, código de buenas practicas

INDICE

página

PREFACIO

A. RESEÑA HISTORICA

A.1 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), mediante el Sistema 1 u Adopción, durante los meses de junio a julio del 2006, utilizando como antecedente a la Norma ISO/IEC 17799:2005 Information technology – Code of practice for information security management.

A.2 El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) presentó a la Comisión de Reglamentos Técnico y Comerciales -CRT-, con fecha 2006-07-21, el PNTP-ISO/IEC 17799:2006 para su revisión y aprobación; siendo sometido a la etapa de Discusión Pública el 2006-11-25. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información**, 2ª Edición, el 22 de enero del 2007.

A.3 Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	EAN PERU
Presidente	Marco Suárez
Secretaria	Mary Wong

ENTIDAD	**REPRESENTANTE**
DISTRIBUIDORA MAYORISTA SYMBOL S.A.	Deyanira Villanueva

DROKASA PERU S.A.	Juan Aquije
E. WONG S.A. FOLIUM S.A.C.	Marcela Aparicio Roberto Huby
ITS CONSULTANTS S.A.C.	Ricardo Dioses
IBC SOLUTIONS PERU S.A.C.	Daniella Orellana
OFICINA DE NORMALIZACION PREVISIONAL	Roberto Puyó
PERU SECURE E-NET S.A.C	Pablo Omonte
PONT. UNIV. CATOLICA DEL PERU	Viktor Khlebnikov Willy Carrera
PRESIDENCIA DEL CONSEJO DE MINISTROS	César Vilchez Max Lazaro
SUPERMERCADOS PERUANOS S.A.	David Mongrut
TECNOLOGÍA FLEXOGRAFICA S.A.	Raúl Adriazola
TRANSPORTE CONFIDENCIAL DE INFORMACIÓN S.A. - TCI	Renzo Alcántara
UNILEVER ANDINA PERU S.A.	Ursula Toyofuku
EAN PERU	Milagros Dávila Tatiana Peña

---oooOooo---

INTRODUCCION

¿Qué es la seguridad de la Información?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información esta expuesta a un mayor rango de amenazas y vulnerabilidades.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

¿Por qué es necesaria la seguridad de información?

La información y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización. Definir, realizar, mantener y mejorar la seguridad de información, pueden ser esencial para mantener la competitividad, flujo de liquidez, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez mas, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de

daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de información es importante en negocios tanto del sector publico como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes publicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

1. La primera fuente procede de la valoración de los riesgos de la organización, tomando en cuenta los objetivos y estrategias generales del negocio. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

2. La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

3. La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad.

Los resultados de ésta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos.

Las evaluaciones de riesgos deben repetirse periódicamente para tener en cuenta cualquier cambio que pueda influir en los resultados de la evaluación.

Mayor información sobre las evaluaciones de riesgos pueden ser encontradas en el inciso 4.1 "Evaluando los riesgos de seguridad"

Selección de controles

Una vez que los requisitos de seguridad han sido identificados y las decisiones para el tratamiento de riesgos han sido realizadas, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de controles o de nuevos controles que pueden diseñarse para cubrir adecuadamente las necesidades específicas. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio para la identificación y clasificación de riesgos, las opciones para el tratamiento de estos y la gestión general de riesgos aplicable a la organización. Así mismo, debe ser sujeto a toda regulación y legislación nacional e internacional.

Ciertos controles expuestos en este documento, pueden considerarse como principios que guían la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Estos se explican en más detalle en el siguiente inciso denominado "Punto de partida de la seguridad de la información".

Mayor información sobre la selección de controles y otros riesgos pueden ser encontradas en el inciso 4.2. " Tratando riesgos de seguridad".

Punto de partida de la seguridad de la información

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) la protección de los datos de carácter personal y la intimidad de las personas (véase el inciso 15.1.4);

b) la salvaguarda de los registros de la organización (véase el inciso 15.1.3);

c) los derechos de la propiedad intelectual (véase el inciso 15.1.2).

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

a) la documentación de la política de seguridad de la información (véase el inciso 5.1.1);

b) la asignación de responsabilidades de seguridad (véase el inciso 6.1.3);

c) la formación y capacitación para la seguridad de la información (véase el inciso 8.2.2);

d) el procedimiento correcto en las aplicaciones (véase el inciso 12.2);

e) la gestión de la vulnerabilidad técnica (véase el inciso 12.6);

f) la gestión de la continuidad del negocio (véase el inciso 14);

g) el registro de las incidencias de seguridad y las mejoras (véase el inciso 13.2).

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

Factores críticos de éxito

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización:

a) una política, objetivos y actividades que reflejen los objetivos del negocio de la organización;

b) un enfoque para implantar, mantener, monitorear e improvisar la seguridad que sea consistente con la cultura de la organización;

c) el apoyo visible y el compromiso de la alta gerencia;

d) una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;

e) la convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados;

f) la distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas;

g) aprovisionamiento para financiar actividades de gestión de seguridad de la información;

h) la formación y capacitación adecuadas;

i) establecer un efectivo proceso de gestión de incidentes de la seguridad de información;

j) un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

Desarrollo de directrices propias

Este código de buenas prácticas puede verse como punto de partida para desarrollar la gestión específica de la seguridad en una organización. Pueden no ser aplicables todas las recomendaciones y controles de este código. Incluso pueden requerirse controles adicionales que este documento no incluye. Cuando esto suceda puede ser útil mantener referencias cruzadas que faciliten la comprobación de la conformidad a los auditores y otros asociados de la organización.

EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La norma puede servir como una guía practica para desarrollar estándares organizacionales de seguridad y practicas efectivas de la gestión de seguridad. Igualmente, permite proporcionar confianza en las relaciones entre organizaciones. Las recomendaciones que se establecen en esta norma deberían elegirse y utilizarse de acuerdo con la legislación aplicable en la materia.

2. TÉRMINOS Y DEFINICIONES

Para los fines de esta norma son de aplicación las definiciones siguientes:

2.1 **activo:** Algo que tenga valor para lo organización. [ISO/IEC 13335-1:2004]

2.2 **control:** Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

NOTA: Control es también usado como sinónimo de salvaguardia o contramedida.

2.3 **pauta:** Descripción que aclara que es lo que se debe hacer y como se hace, con el fin de alcanzar los objetivos planteados en las políticas. [ISO/IEC 13335-1:2004]

2.4 **instalaciones de proceso de información:** Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

2.5 **seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

2.6 **evento de seguridad de información:** Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 18044-1:2004]

2.7 **incidente de seguridad de información:** Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. [ISO/IEC TR 18044:2004]

2.8 **política**: Dirección general y formal expresada por la gerencia.

2.9 **riesgo:** Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guide 73:2002]

2.10. **análisis del riesgo:** Uso sistemático de la información para identificar fuentes y estimar el riesgo. [ISO/IEC Guide 73:2002]

2.11. **evaluación del riesgo:** Proceso general de análisis y evaluación del riesgo. [ISO/IEC Guide 73:2002]

2.12. **valoración del riesgo:** Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este. [ISO/IEC Guide 73:2002]

2.13. **gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización considerando el riesgo.

NOTA: Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

[ISO/IEC Guide 73:2002]

2.1.4. **tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo. [ISO/IEC Guide 73:2002]

2.15. **terceros:** Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión. [ISO/IEC Guide 73:2002]

2.16. **amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO/IEC 13335-1:2004]

2.17. **vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o mas amenazas. [ISO/IEC 13335-1:2004]

3. ESTRUCTURA DE ESTE ESTANDAR

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

3.1 Cláusulas

Cada cláusula contiene un numero de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el numero de categorías principales de seguridad incluidas en cada cláusula) son:

a) Política de seguridad (1);

b) Organizando la seguridad de información (2);

c) Gestión de activos (2);

d) Seguridad en recursos humanos (3);

e) Seguridad física y ambiental (2);

f) Gestión de comunicaciones y operaciones (10);

g) Control de acceso (7);

h) Adquisición, desarrollo y mantenimiento de sistemas de información (6);

i) Gestión de incidentes de los sistemas de información (2);

j) Gestión de la continuidad del negocio (1);

k) Cumplimiento (3)

NOTA: El orden de las cláusulas en este estándar no implica su importancia. Dependen de las circunstancias, todas las cláusulas pueden ser importantes, por lo tanto cada organización que aplica este estándar debe identificar cláusulas aplicables, que tan importantes son y sus aplicaciones para procesos de negocios individuales. Igualmente, todas las listas de este estándar no se encuentran en orden de prioridad a menos que se notifique lo contrario.

3.2 Categorías principales de seguridad

Cada categoría principal de seguridad contiene:

a) un objetivo de control declarando lo que se debe alcanzar.

b) uno o mas controles que pueden ser aplicados para alcanzar el objetivo de control.

Las descripciones del control son estructuradas de la siguiente manera:

Control

Define específicamente la declaración de control para satisfacer el objetivo de control.

Guía de implementación

Provee información mas detallada para apoyar la implementación del control y conocer el objetivo de control. Algunas guías pueden no ser convenientes para todos los casos, por lo tanto algunas otra formas de implementar el control pueden ser mas apropiadas.

Otra información

Provee información adicional que pueda ser necesaria, por ejemplo consideraciones legales y referencias de otros estándares.

4. EVALUACION Y TRATAMIENTO DEL RIESGO

4.1 Evaluando los riesgos de seguridad

La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un numero de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debe incluir un alcance sistemático sobre la estimación de la magnitud del riesgo (análisis del riesgo) y sobre el proceso de comparar el riesgo estimado con el criterio para determinar el significado de los riesgos (valoración del riesgo).

Las evaluaciones del riesgo deben ser realizadas periódicamente para incluir los cambios en los requerimientos del sistema y en la situación del riesgo, por ejemplo en los activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando cambios significativos ocurran. Estas evaluaciones del riesgo deben ser emprendidas de una forma metódica, capaz de producir resultados comparables y reproducibles.

La evaluación de la información del riesgo de seguridad debe tener un alcance claro y definido para que este sea efectivo y debe incluir relaciones con las evaluaciones del riesgo en otras áreas, si es apropiado.

El alcance de la evaluación del riesgo puede ser para toda la organización, partes de ella, un sistema individual de información, componentes específicos del sistema o servicios donde esto puede ser utilizado, realista y provechoso. Ejemplos de metodologías de la evaluación del riesgo son discutidas en ISO/IEC TR 13335-3 (Guía para la gestión en la seguridad de tecnologías de información).

4.2 Tratando riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, la organización debe decidir el criterio para determinar si es que los riesgos son aceptados o no. Los riesgos pueden ser aceptados si, por

ejemplo, se evalúa que el riesgo es menor o que el costo de tratarlo no es rentable para la organización. Estas decisiones deben ser grabadas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo, se necesita realizar una decisión del tratamiento del riesgo. Posibles opciones para el tratamiento del riesgo incluye:

a) Aplicar controles apropiados para reducir riesgos.

b) Riesgos aceptados objetivamente y con conocimiento, satisfaciendo claramente el criterio para la aceptación del riesgo y la política de la organización.

c) Evitar riesgos no permitiendo realizar acciones que puedan causar que estos riesgos ocurran.

d) Transferir los riesgos asociados a terceros como son los proveedores y aseguradores.

Para esos riesgos donde la decisión del tratamiento del riesgo ha sido aplicado a controles apropiados, esos controles deben ser seleccionados e implementados para conocer los requerimientos identificados por una evaluación de riesgos. Los controles deben asegurarse de que los riesgos son reducidos a un nivel aceptable tomando en cuenta:

a) Exigencias y coacciones de las legislaciones y regulaciones nacionales e internacionales.

b) Objetivos organizacionales.

c) Exigencias y coacciones operacionales.

d) Costo de la implementación y operación en relación con los riesgos que serán reducidos y siendo proporcional a las exigencias y coacciones de la organización.

e) La necesidad para balancear la inversión en implementación y operación de los controles contra el daño que pueda resultar de las fallas en la seguridad.

Los controles pueden ser seleccionadas de este estándar o de otro conjunto de controles o de nuevos controles que pueden ser designados para conocer las necesidades especificas de la organización. Como un ejemplo, 10.1.3 describe como los deberes deben ser segregados para prevenir fraude y error. Puede que no sea posible para las organizaciones pequeñas segregar todos sus deberes por lo que pueden ser necesarias otras formas de alcanzar el mismo objetivo de control. Otro ejemplo, 10.10 describe como el uso del sistema puede ser monitoreado y la

evidencia recolectada. Los controles descritos, como el registro de eventos, pueden entrar en conflicto con la legislación actual, en lo que se refiere a la protección de la privacidad para clientes o en el establecimiento de trabajo.

Los controles en la seguridad de información deben ser considerados en los sistemas y en las especificaciones de las exigencias de los proyectos así como en la etapa de diseño. Las fallas pueden resultar en costos adicionales y en soluciones menos efectivas y posiblemente, en el peor de los casos, inhabilidad para alcanzar una seguridad adecuada.

Se debe tener en cuenta que ningún conjunto de controles puede alcanzar completa seguridad y que una gestión adicional deberá implementarse para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar las necesidades de la organización.

5. POLÍTICA DE SEGURIDAD

5.1 Política de seguridad de la información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

5.1.1 Documento de política de seguridad de la información

Control

La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.

Guía de implementación

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como mínimo la siguiente información:

a) una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información (véase el capítulo de Introducción);

b) el establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información;

c) un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo;

d) una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo:

1) conformidad con los requisitos legislativos y contractuales;

2) requisitos de formación en seguridad;

3) gestión de la continuidad del negocio;

4) consecuencias de las violaciones de la política de seguridad;

e) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad;

f) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

Otra información

La política de seguridad debe ser parte de un documento general de la política empresarial. Se debe tener cuidado al distribuir la política de seguridad fuera de la organización con el fin de no compartir información confidencial.

5.1.2 Revisión y evaluación

Control

La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.

Guía de implementación

La política debería tener un propietario que sea responsable del desarrollo, revisión y evaluación de la política de seguridad. La revisión debe incluir oportunidades de evaluación para mejorar la política de seguridad de información de la organización y un acercamiento a la gestión de seguridad de información en respuesta a los cambios del ambiente organizacional, circunstancias del negocio, condiciones legales o cambios en el ambiente técnico.

La revisión de la política de seguridad de información debe tomar en cuenta los resultados de las revisiones de la gestión. Deben existir procedimientos definidos de la gestión de revisión, incluyendo un calendario o periodo de revisión.

El input para la revisión de la gestión debe incluir información acerca de:

a) retroalimentación sobre terceros interesados;

b) resultados de revisiones independientes (véase el inciso 6.1.8);

c) estado sobre acciones preventivas y correctivas (ver 6.1.8 y 15.2.1);

d) resultados de revisiones de gestión anteriores;

e) desarrollo del proceso y cumplimiento de la política de seguridad de información;

f) cambios que pueden afectar el alcance de la organización para gestionar la seguridad de información, incluyendo cambios al ambiente organizacional, circunstancias del negocio , disponibilidad de recursos, condiciones contractuales, regulatorias y legales o cambios en el ambiente técnico;

g) tendencias relacionadas con amenazas y vulnerabilidades;

h) incidentes reportados de seguridad de información (véase el inciso 13.1);

i) recomendaciones dadas por autoridades relevantes (véase el inciso 6.1.6).

El output para la revisión de la gestión debe incluir información acerca de:

a) mejoras en el alcance de la organización para gestionar seguridad de información y sus procesos;

b) mejoras en los objetivos de control y los controles;

c) mejoras en la asignación de recursos y/o responsabilidades.

Un registro de la revisión de la gestión debe ser mantenido.

Aprobación gerencial para la política revisada debe ser obtenida.

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

6.1 Organización interna

OBJETIVO: Gestionar la seguridad de la información dentro de la organización.

Debería establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

Es conveniente organizar foros de gestión adecuados con las gerencias para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implantación de la seguridad en toda la organización.

Si fuera necesario, debería facilitarse el acceso dentro de la organización a un equipo de consultores especializados en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como tener un punto de enlace para tratar las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información.

6.1.1 Comité de gestión de seguridad de la información

Control

La gerencia debe apoyar activamente en la seguridad dentro de la organización a través de direcciones claras demostrando compromiso, asignaciones explicitas y reconocimiento de las responsabilidades de la seguridad de información.

Guía de implementación

Este comité debería realizar las siguientes funciones:

a) asegurar que las metas de la seguridad de información sean identificadas, relacionarlas con las exigencias organizacionales y que sean integradas en procesos relevantes;

b) formular, revisar y aprobar la política de seguridad de información;

c) revisión de la efectividad en la implementación de la política de información;

d) proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad;

e) proveer los recursos necesarios para la seguridad de información;

f) aprobar asignaciones de roles específicos y responsabilidades para seguridad de información a través de la organización;

g) iniciar planes y programas para mantener la conciencia en seguridad de información;

h) asegurar que la implementación de los controles de la seguridad de información es coordinada a través de la organización. (véase el inciso 6.1.2).

La gerencia debe identificar las necesidades de asesoría especialista ya sea interna o externa, revisando y coordinando los resultados de la esta a través de la organización.

Dependiendo del tamaño de la organización, estas responsabilidades pueden ser manejadas por un forum gerencial dedicado o por un cuerpo gerencial existente, como el consejo directivo.

Otra información

Mayor información esta contenida en ISO/IEC 13335-1:2004.

6.1.2 Coordinación de la seguridad de la información

Control

La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la organización con roles relevantes y funciones de trabajo.

Guía de implementación

Comúnmente, la coordinación de la seguridad de información debe implicar la cooperación y la colaboración de gerentes, usuarios, administradores, diseñadores de la aplicación, personal de auditoria y seguridad, y habilidades especiales en áreas como seguros, tramites legales, recursos humanos, tecnología de la información o gestión del riesgo. Esta actividad debe:

a) asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad;

b) identificar como manejar los no cumplimientos;

c) aprobar metodologías y procesos para seguridad de información, como por ejemplo la evaluación del riesgo y la clasificación de información;

d) identificar cambios significativos de amenazas y exposición de información;

e) evalúa la adecuación y coordina la implantación de los controles de seguridad de la información;

f) promocionar efectivamente educación, entrenamiento y concientizar en seguridad de información, a través de la organización;

g) evaluar información de seguridad recibida de monitorear y revisar los incidentes de seguridad de información y recomendar acciones apropiadas en respuesta para identificar incidentes de seguridad de información.

Si la organización no usa un grupo funcional separado, porque ese grupo no es apropiado para el tamaño de la organización, las acciones descritas anteriormente deben ser tomadas por otro cuerpo gerencial ajustable o por un gerente individual.

6.1.3 Asignación de responsabilidades sobre seguridad de la información

Control

Deberían definirse claramente las responsabilidades.

Guía de implementación

La asignación de responsabilidades sobre seguridad de la información deben hacerse en concordancia con la información de la política de seguridad (véase capitulo 4). Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas. Esta asignación, debería completarse, dónde sea necesario, con una guía más detallada para ubicaciones, sistemas o servicios específicos. Deberían definirse claramente las responsabilidades locales para activos físicos y de información individualizados y los procesos de seguridad como, por ejemplo, el plan de continuidad del negocio.

Los propietarios de los activos de información pueden delegar sus responsabilidades de seguridad en directivos a título individual o en proveedores de servicios. Sin embargo, el propietario sigue manteniendo la responsabilidad última sobre la seguridad del activo y debería estar capacitado para determinar que cualquier responsabilidad delegada se ha cumplido correctamente.

Es esencial que se establezcan claramente las áreas de las que cada directivo es responsable; en particular deberían establecerse las siguientes:

a) deberían identificarse claramente los activos y los procesos de seguridad asociados con cada sistema específico;

b) debería nombrarse al responsable de cada activo o proceso de seguridad, y deberían documentarse los detalles de esta responsabilidad;

c) deberían definirse y documentarse claramente los niveles de autorización.

Otra información

Muchas organizaciones nombran un director de seguridad de la información como el responsable del desarrollo e implantación de la seguridad y para dar soporte a la identificación de las medidas de control.

Sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control suele recaer en ciertos directivos. Una práctica habitual consiste en designar un propietario de cada activo de información, que se convierte así en responsable de su seguridad cotidiana.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información

Control

Debería establecerse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.

Guía de implementación

Deberían considerarse los siguientes controles:

a) los nuevos medios deberían tener la aprobación adecuada de la gerencia de usuario, autorizando su propósito y uso. También debería obtenerse la aprobación del directivo responsable del mantenimiento del entorno de seguridad del sistema de información local, asegurando que cumple con todas las políticas y requisitos de seguridad correspondientes;

b) dónde sea necesario, se debería comprobar que el hardware y el software son compatibles con los demás dispositivos del sistema;

c) debería autorizarse y evaluarse el uso de medios informáticos personales, como laptops o aparatos móviles, para el tratamiento de la información de la organización así como los controles necesarios, ya que pueden introducir nuevas vulnerabilidades.

6.1.5 Acuerdos de confidencialidad

Control

Requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente.

Guía de implementación

Confidencialidad o acuerdos de no divulgación deben anexar los requerimientos para proteger información confidencial usando términos ejecutables legales. Para identificar requerimientos de confidencialidad o acuerdos de no divulgación, se deben considerar los siguientes elementos:

a) una definición de la información a ser protegida;

b) duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente;

c) acciones requeridas cuando un acuerdo sea finalizado;

d) responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información;

e) propiedad de la información, secretos del comercio y de la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;

f) la permisión de utilizar información confidencial y los derechos del signatario para usar la información;

g) el derecho de auditar y monitorear actividades que impliquen información confidencial;

h) procesos para notificar y reportar acceso desautorizado a aberturas de información confidencial;

i) términos para que la información sea retornada o destruida en la cesación del acuerdo; y

j) acciones prevista que se tomará en caso de una abertura de este acuerdo.

Basado en los requerimientos de la seguridad de una organización, otros elementos pueden ser necesarios en una acuerdo de confidencialidad o de no-acceso.

Los acuerdos de confidencialidad y de no-acceso deben conformarse con todas las leyes aplicables y las regulaciones para la jurisdicción a la cual aplica (véase el inciso 15.1.1).

Los requerimientos para acuerdos de confidencialidad y de no-acceso deben ser revisados periódicamente y cuando ocurran cambios que influyan en estos requerimientos.

Otra información

Los acuerdos de confidencialidad y de no-acceso pretejen información organizacional e informan a los signatarios de sus responsabilidades a proteger, usando y accesando información de forma responsable y autorizada.

Puede ser necesario para una organización, usar diferentes formas de acuerdos de confidencialidad o de no-acceso en diferentes circunstancias.

6.1.6 Contacto con autoridades

Control

Deben ser mantenidos contactos apropiados con autoridades relevantes.

Guía de implementación

Las organizaciones deben de tener procedimientos instalados que especifiquen cuando y por que autoridades deben ser contactados y como los incidentes identificados en la seguridad de información deben ser reportados de una manera oportuna si se sospecha que las leyes han sido rotas.

Las organizaciones bajo ataque desde el Internet pueden necesitar de terceros (proveedor del servicio de Internet u operadores de telecomunicaciones) para tomar acción contra la fuente de ataque.

Otra información

Mantener dichos contactos puede ser un requerimiento para apoyar la gestión de los incidentes de seguridad de la información (sección 13.2) o la continuidad del negocio y la contingencia del planeamiento (sección 14). Contactos con cuerpos regulatorios son también útiles para anticiparse y prepararse a próximos cambios en la ley o en las regulaciones, que deben ser seguidos por la organización. Contactos con otras autoridades incluyen utilidades, servicios de emergencia, seguridad y salud, como por ejemplo los bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (en conexión con la línea de ruta y la disponibilidad), proveedores de agua (en conexión con instalaciones de refrigeración para el equipo).

6.1.7 Contacto con grupos de interés especial

Control

Deben mantenerse contactos apropiados con grupos de interés especial u otros especialistas en foros de seguridad y asociaciones profesionales.

Guía de implementación

Membresía en grupos de interés especial o foros deben ser considerados debido a que:

a) mejorar el conocimiento sobre mejores practicas y estar actualizado con información relevante de seguridad;

b) asegurar que el entendimiento del ambiente de seguridad de información es actual y completo;

c) recibir alertas de detección temprana, advertencias y parches que para los ataques y a las vulnerabilidades;

d) ganar acceso a consejos especializados de seguridad de información;

e) compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades;

f) proveer puntos de enlaces convenientes cuando se trata con información de incidentes de seguridad (véase el inciso 13.2.1).

Otra información

Acuerdos para compartir información pueden ser establecidos para mejorar la cooperación y coordinación de temas de seguridad. Estos acuerdos deben identificar requerimientos para la protección de información sensible.

6.1.8 Revisión independiente de la seguridad de la información.

Control

El alcance de la organización para gestionar la seguridad de información y su implementación (objetivos de control, controles, políticas, procesos y procedimientos para seguridad de información) deben ser revisados independientemente en intervalos planificados o cuando cambios significativos a la puesta en marcha de la seguridad ocurran.

Guía de implementación

La revisión independiente debe ser iniciado por la gerencia. Esta revisión independiente es necesaria para asegurar la continua conveniencia, suficiencia y eficacia del alcance de la organización hacia la gestión de información de seguridad. La revisión debe incluir oportunidades de evaluación para mejorar y la necesidad de cambios para el acercamiento a la seguridad, incluyendo la política y los objetivos de control.

Esta revisión debe ser llevado a acabo por individuos independientemente del área bajo revisión. Los individuos que llevan a cabo estas revisiones deben de tener las habilidades y la experiencia apropiada.

Los resultados de la revisión independiente deben ser registrados y reportados a la gerencia que inicio la revisión. Estos registros deben mantenerse.

Si la revisión independiente identifica que el alcance de la organización o la implementación de la gestión de seguridad de información es inadecuada o no complaciente con la dirección de seguridad de información establecida en la política, la gerencia debe considerar acciones correctivas.

Otra información

El área, cuyos gerentes deben revisar regularmente, pueden ser revisados también independientemente. Las técnicas de revisión pueden incluir entrevistas a la gerencia, comprobación de expedientes o revisión de los documentos de la política de seguridad. ISO 19011:2002, pautas para la calidad y/o revisión de los sistemas de la gestión ambiental, pueden proveer una guía de ayuda para llevar a cabo revisiones independientes, incluyendo establecimiento e implementación de un programa de revisión. El inciso 15.3 especifica controles relevantes para la revisión independiente de los sistemas de información operacional y el uso se herramientas para auditar sistemas.

6.2 Seguridad en los accesos de terceras partes

OBJETIVO: Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no deben ser reducidas por la introducción de un servicio o producto externo.

Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.

Cuando el negocio requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato: con la tercera parte.

6.2.1 Identificación de riesgos por el acceso de terceros

Control

Los riesgos a la información de la organización y a las instalaciones del procesamiento de información desde los procesos del negocio que impliquen a terceros deben ser identificados y se debe implementar controles apropiados antes de conceder el acceso.

Guía de implementación

Cuando es necesario permitir el acceso a las instalaciones del procesamiento de información o a la información de una organización a un tercero, una evaluación el riesgo (véase también la sección 4) debe ser llevada a cabo para identificar cualquier requisito para controles específicos. La identificación de los riesgos relacionados con el acceso a terceros debe de tomar en cuenta los siguientes puntos:

a) Las instalaciones del procesamiento de la información a la que terceros requieren acceso;

b) El tipo de acceso que terceros tendrán a la información y a las instalaciones del procesamiento de infamación:

1) acceso físico, por ejemplo oficinas o salas de ordenadores;

2) acceso lógico, por ejemplo la base de datos de la organización o sistemas de información;

3) conectividad de red entre la organización y terceros, por ejemplo la conexión permanente o acceso remoto;

4) si el acceso esta ocurriendo en el sitio o fuera de el;

c) el valor y la sensibilidad de la información implicada, y es critico para operaciones de negocios;

d) los controles necesarios para proteger la información que no debe ser accesible a terceros;

e) el personero externo implicado en maniobrar la información de la organización;

f) como la organización o el personero autorizado para tener acceso puede ser identificado, la autorización verificada y que tan seguido necesita ser reconfirmada;

g) los diferentes significados y controles empleados por terceros cuando guarde, procese, comunique, comparta e intercambia información;

h) el impacto del acceso no disponible a terceros cuando sea requerido, y de terceros ingresando o recibiendo información inexacta o engañosa;

i) practicas y procedimientos para lidiar con incidentes y daños potenciales en la seguridad de información, y los términos y condiciones para continuar con el acceso a terceros en el caso de un incidente en la seguridad de información;

j) requisitos legales y regulatorios u otras obligaciones contractuales relevantes a terceros que deben ser tomadas en cuenta;

k) como los intereses de las partes interesadas pueden ser afectados por los acuerdos.

El acceso por terceras personas a la información de la organización no debe ser provista hasta que se haya implementado los controles apropiados y que estros sean factibles, un contrato ha sido firmado definiendo los términos y condiciones para la conexión o el acceso y los arreglos de trabajo. Generalmente, todos los requerimientos resultantes del trabajo con terceros o de los controles internos deben ser reflejados con el visto bueno de ellos (véase también 6.2.2 y 6.2.3).

Debemos asegurarnos que las terceras personas estén enteradas de sus obligaciones y que acepten las responsabilidades que implica acceder, procesar, comunicar o manejar la información de la organización y las instalaciones del procesamiento de información.

Otra información

La información puede ser puesta en riesgo por terceros con una inadecuada gestión de seguridad. Los controles deben ser identificados y aplicados para administrar el acceso a terceros a las instalaciones de procesamiento de información. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, acuerdos de no-acceso pueden ser usados.

Las organizaciones pueden enfrentar riesgos asociados con los procesos inter-organizacionales, gestión y comunicación, si un alto nivel de outsourcing es aplicado o donde existan diversas terceras partes implicadas.

Los controles 6.2.2 y 6.2.3 cubren diferentes acuerdos con terceras partes, incluyendo:

a) proveedores de servicios, como ISPs, proveedores de red, servicio telefónico, mantenimiento y servicios de apoyo;

b) servicios de gestión de seguridad;

c) clientes;

d) outsourcing de instalaciones y/o operaciones, como sistemas de información de la información, servicios de recolección de datos, operaciones de central de llamadas;

e) consultores gerenciales y de negocios, y auditores;

f) proveedores de productos de software y servicios de información;

g) limpieza, cafetería y otros servicios de apoyo externo;

h) personal temporal, estudiantes en practicas u otros contratados por tiempo limitado.

Estos acuerdos pueden ayudar a reducir el riesgo asociado con terceros.

6.2.2 Requisitos de seguridad cuando sea trata con clientes

Control

Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la organización.

Guía de implementación

Los siguientes términos deben ser considerados para ser anexados a la seguridad antes de dar a los clientes acceso a los activos de seguridad (dependiendo del tipo y la extensión del acceso dado, no todos se aplican):

a) protección de activos, incluyendo:

1) procedimientos para proteger los activos de la organización, incluida la información y el software;

2) procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos, por ejemplo, una pérdida o modificación de datos;

3) medidas de integridad;

4) restricciones en la copia o divulgación de la información;

b) la descripción del servicio o producto disponible;

c) las diferentes razones, requerimientos y beneficios para el acceso del cliente;

d) acuerdos sobre control de accesos, incluyendo:

1) los métodos de acceso permitidos, así como el control y uso de identificadores únicos, como número de identificación ID y contraseñas;
2) el procedimiento de autorización del acceso y privilegios a los usuarios;

3) una declaración de que todo acceso que no esta explícitamente autorizado es prohibido;

4) un proceso para revocar el derecho de acceso o interrumpir la conexión entre sistemas;

e) arreglos para reportar, notificar e investigar inexactitudes de información (como detalles personales), incidentes y aberturas en la seguridad de información;

f) una descripción de cada servicio a ser disponible;

g) el nivel de servicio;

h) el derecho para controlar y revocar cualquier actividad relacionado con los activos de la organización;

i) las respectivas responsabilidades de la organización y de los clientes;

j) las responsabilidades en materia de legislación por ejemplo sobre protección de datos personales, teniendo especialmente en cuenta los diferentes sistemas legales nacionales si el contrato implica la cooperación con organizaciones de otros países (véase también el inciso 15.1);

k) los derechos de propiedad intelectual, protección contra copias (véase el inciso 15.1.2.) y protección en tareas de colaboración (véase también el inciso 6.1.5).

Otra información

Los requerimientos de seguridad relacionados con el acceso a los activos de la organización de los clientes pueden variar considerablemente dependiendo de las instalación del procesamiento de información y la información a la que se accede. Estos requerimientos en la seguridad pueden ser anexados usando acuerdos con los clientes, que contienen todos los riesgos identificados y los requerimientos de seguridad.

Los acuerdos con terceros también pueden implicar a otras partes. Estos acuerdos garantizando acceso a terceros deben incluir permisos para la designación de otras partes y condiciones para su acceso y su inclusión.

6.2.3 Requisitos de seguridad en contratos de outsourcing

Control

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, debe cubrir todos los requisitos de seguridad relevantes.

Guía de implementación

El acuerdo debe asegurar que no exista desentendimiento entre la organización y las terceras partes. Las organizaciones deben satisfacerse en cuanto a la indemnidad de los terceros.

Los siguientes términos deben ser considerados para inclusión en el acuerdo con el fin de satisfacer los requisitos identificados de seguridad (véase el inciso 6.2.1).

a) la política de información de seguridad;

b) los controles que aseguren la protección del activo, incluyendo:

1) procedimientos para proteger los activos organizacionales, incluyendo información, software y hardware;

2) controles cualquiera de protección física requerida y mecanismos;

3) controles para asegurar la protección contra software malicioso;

4) procedimientos para determinar si es que se compromete el activo, como la perdida o modificación de la información, software y hardware, ha ocurrido;

5) controles que aseguran el retorno o la destrucción de información y activos al final de o de un tiempo acordado durante el acuerdo;

6) confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante (véase el inciso 2.1.5) de los activos;

7) restricciones para copiar y divulgar información y el uso de acuerdos de confidencialidad;

c) capacitación en los métodos, procedimientos y seguridad para usuario y administrador;

d) asegurar el conocimiento del usuario para temas y responsabilidades de la seguridad de información;

e) disposición para transferir personal, cuando sea apropiado;

f) responsabilidades con respecto a la instalación y el mantenimiento del hardware y software;

g) una clara estructura y formatos de reportes;

h) un claro y especificado proceso de cambio de gestión;

i) política de control de acceso, cubriendo:

1) las diferentes razones, requerimientos y beneficios que hacen el acceso por terceros necesario;

2) métodos permitidos de acceso y el control y uso de identificadores únicos como ID de usuario y contraseñas;

3) un proceso autorizado para acceso de usuarios y los privilegios;

4) un requerimiento para mantener una lista de individuos autorizados a usar el servicio que ha sido disponible y cual son sus derechos y privilegios respecto a su uso;

5) una declaración de que todos los accesos que no son explícitamente autorizados son prohibidos;

j) arreglos para reportar, notificar e investigar incidentes de la seguridad de información y aperturas de seguridad, como violaciones de los requerimientos establecidos en el acuerdo;

k) una descripción del producto o servicio ha ser provisto y una descripción de la información ha ser disponible de acuerdo con su clasificación de seguridad (véase el inciso 7.2.1);

l) el objetivo de nivel de servicio y los niveles de no aceptación;

m) la definición del criterio de comprobación del funcionamiento, su control y su reporte;

n) el derecho de controlar y revocar cualquier actividad relacionada con los activos de la organización;

o) el derecho para auditar responsabilidades definidas en el acuerdo, para que dichas auditorias sean llevadas a cabo por terceros y para enumerar los derechos estatutarios de los auditores;

p) el establecimiento de un proceso de escalamiento para resolver problemas;

q) requisitos continuos de servicio, incluyendo medidas para la disponibilidad y la confiabilidad, en concordancia con las prioridades de negocio de la organización;

r) las respectivas responsabilidades de las partes del acuerdo;

s) responsabilidades con respecto a temas legales y como se asegura que los requerimientos legales sean conocidos, como por ejemplo la legislación de protección de datos, considerar especialmente diversos sistemas legislativos nacionales si el

acuerdo implica la cooperación con organizaciones de otros países (véase el inciso 6.1.5);

t) derechos de propiedad intelectual y de asignación de copyright y protección de cualquier otro trabajo de colaboración (véase también 6.1.5);

u) implicancias entre los sub-contratantes y terceros, y los controles de seguridad que estos sub-contratantes necesitan implementar;

v) condiciones para la renegociación/terminacion de los acuerdos:

1) un plan de contingencia debe llevarse a cabo en caso de que cualquiera de las partes desee cortar relaciones antes del termino de los acuerdos;

2) renegociación de los acuerdos si los requisitos de seguridad de la organización cambian;

3) documentación actual de la lista de activos, licencias, acuerdos o derechos relacionados con ellos.

Otra información

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de terceros. Es por eso que es necesario tener cuidado al identificar riesgos y requisitos de seguridad (véase también 6.2.1) en los acuerdos. Donde sea necesario, los controles y procedimientos requeridos pueden ser extendidos en el plan de gestión de seguridad.
Si la gestión de seguridad de información es externa, los acuerdos deben anexar como es que las terceras partes garantizaran una seguridad adecuada sera mantenida, como esta definida en la evaluación de riesgos, y como la seguridad será adaptada para identificar y tratar con cambios en los riesgos.

Algunas de las diferencias entre el outsourcing y otro tipo de servicio de terceros incluye las preguntas de responsabilidad, planeamiento del periodo de transición y la potencial interrupción de operaciones durante este periodo, arreglos del planeamiento de contingencia y las revisiones de la diligencia debida, y la colección y gestión de los incidentes de seguridad de información. Por lo tanto, es importante que la organización planifique y gestione la transición con un acuerdo de outsourcing y que tenga procesos adecuados para manejar los cambios y las renegociaciones/terminaciones de los acuerdos.

Los procedimientos para el proceso continuo en el caso de que las terceras partes sean incapaces de suministrar sus servicios, necesitan ser considerados en el acuerdo con el fin de evitar cualquier retraso en hallar servicios de reemplazo.

Los acuerdos con terceros deben incluir a otras partes. Acuerdos en los cuales se garantice acceso a terceros debe incluir permiso para designar otras partes elegibles y condiciones para su acceso e inclusión.

Generalmente, los acuerdos son desarrollados primariamente por la organización. Puede haber ocasiones en algunas circunstancias donde el acuerdo pueda ser desarrollado e impuesto a una organización por un tercero. La organización necesita asegurar que su propia seguridad no esta necesariamente impactada por requisitos de una tercera persona estipulado en acuerdos impuestos.

7. CLASIFICACIÓN Y CONTROL DE ACTIVOS

7.1 Responsabilidad sobre los activos

OBJETIVO: Mantener una protección adecuada sobre los activos de la organización.

Todos los activos deben ser considerados y tener un propietario asignado.

Deberían identificarse los propietarios para todos los activos importantes, y se debería asignar la responsabilidad del mantenimiento de los controles apropiados. La responsabilidad de la implantación de controles debería delegarse. Pero la responsabilidad debería mantenerse en el propietario designado del activo.

7.1.1 Inventario de activos

Control

Todos los activos deben se claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.

Guía de implementación

Una organización debe identificar todos los activos y la documentación de importancia de ellos. El inventario de activos debe incluir toda la información necesaria con el fin de

recuperarse de un desastre, incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencia y el valor dentro del negocio. El inventario no debe duplicar otros inventarios sin necesidad , pero debe esta seguro de que el contenido se encuentra alineado.

En adición, los propietarios (véase el inciso 7.1.2) y la clasificación de la información (véase el inciso 7.2) debe ser aceptada y documentada para cada uno de los activos. Basado en la importancia del activo, su valor dentro del negocio y su clasificación de seguridad, se deben identificar niveles de protección conmensurados con la importancia de los activos.

Otra información

Existen muchos tipos de activos, incluyendo:

a) activos de información: archivos y bases de datos, documentación del sistema, manuales de los usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada;

b) activos de software: software de aplicación, software del sistema, herramientas y programas de desarrollo;

c) activos físicos: equipo de computo, equipo de comunicaciones, medios magnéticos (discos y cintas) u otro equipo técnico;

d) servicios: servicios de computo y comunicaciones, servicios generales (calefacción, alumbrado, energía, aire acondicionado);

e) personas, y sus calificaciones, habilidades y experiencia;

f) intangibles, como la reputación y la imagen organizacional.

Los inventarios de los activos ayudan a asegurar que se inicie su protección eficaz, pero también se requiere para otros propósitos de la organización, por razones de prevención laboral, pólizas de seguros o gestión financiera. El proceso de constituir el inventario de activos es un aspecto importante de la gestión de riesgos. Una organización tiene que poder identificar sus activos y su valor e importancia relativos (véase también la sección 4).

7.1.2 Propiedad de los activos

Control

Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización.

Guía de implementación

Los propietarios de los activos deben ser responsables por:

a) asegurar que la información y los activos asociados con las instalaciones de procesamiento de información son apropiadamente clasificadas;

b) definiendo y revisando periódicamente las restricciones de acceso y las clasificaciones, tomando en cuenta políticas de control aplicables.

La propiedad debe ser asignada a:

a) proceso de negocios;

b) un conjunto definido de actividades;

c) una paliación; o

d) un conjunto definido de datos.

Otra información

Tareas de rutina pueden ser delegadas, como la de un custodio que se ocupa de un activo en una base diaria, pero la responsabilidad recae en el propietario.
En sistemas complejos de información, puede ser útil designar un grupo de activos que actúen juntos para proveer una función particular como “services”. En este caso, el propietario del servicio es responsable por la entrega del servicio, incluyendo la funcionalidad de los activos a los cual provee.

7.1.3 Uso adecuado de los activos

Control

Las reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de la información deben ser identificadas, documentados e implementadas.

Guía de implementación

Todos los empleados, contratistas y terceras partes deben de seguir las siguientes reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de información, incluyendo:

a) reglas para correo electrónico y usos de Internet (véase el inciso 10.8);

b) guías para el uso de aparatos móviles, especialmente para el uso fuera de las premisas de la organización (véase el inciso 11.7.1);

Reglas especificas o guías deben ser provistas por la gerencia relevante. Empleados, contratistas y usuarios de terceros usando o teniendo acceso a los activos de la organización deben estar al tanto de los limites existentes para el uso de la información de la organización y de los activos asociados con las instalaciones de procesamiento de información y recursos. Ellos deben ser responsables del uso de cualquier recurso del procesamiento de información y de cualquier otro uso parecido bajo su responsabilidad.

7.2 Clasificación de la información

OBJETIVO: Asegurar un nivel de protección adecuado a los activos de información.

La información debería clasificarse para indicar la necesidad, prioridades y grado de protección.

La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un uso especial. Debería utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas de utilización especial.

7.2.1 Guías de clasificación

Control

La información debería clasificarse en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Guía de implementación

Las clasificaciones de información y otros controles de protección asociados deberían tener en cuenta que el negocio necesita compartir o restringir la información, así como los impactos en la organización asociados a esas necesidades.

Las guías de clasificación deben incluir convenciones para la clasificación inicial y la reclasificación a través del tiempo, en concordancia con algunas políticas de control predeterminadas (véase 11.1.1).

Debe ser responsabilidad del propietario del activo (véase 7.1.2) definir la clasificación de este, revisarlo periódicamente y asegurarse que esta actualizado y en un nivel apropiado. La clasificación debe tomar en cuenta el efecto agregado mencionado en 10.7.2.
Debe darse consideración al numero de categorías de clasificación y los beneficios que se obtendrán de su uso. Esquemas muy complejos pueden ser incómodos y poco rentables de usar o pueden probarse imprácticos. Se debe mantener cuidado al interpretar las etiquetas de clasificación en documentos de otras organizaciones que puedan tener diferentes definiciones para nombres de etiquetas iguales o similares.

Otra información

El nivel de protección puede ser determinado analizando la confidencialidad, integridad y disponibilidad u otro requisito para la información considerada.

La información continuamente deja de ser sensible o critica después de un cierto periodo de tiempo, por ejemplo, cuando la información ha sido hecha publica. Estos aspectos deben ser tomados en cuenta, como la sobre clasificación puede llevar a la implementación de controles innecesarios resultando en gastos adicionales.

Considerando documentos con similares requisitos de seguridad cuando se asigne los niveles de clasificación, pueden ayudar a simplificar las tareas de clasificación.

En general, la clasificación dada como información permite determinar como esta información debe ser maniobrada y protegida.

7.2.2 Marcado y tratamiento de la información

Control

Es importante definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.

Guía de implementación

Los procedimientos para el marcado de la información han de cubrir los activos en formato físico y electrónico.

La salida procedente de los sistemas que traten información clasificada como sensible o crítica deberían llevar una etiqueta de clasificación adecuada (en la salida). El marcado debería reflejar la clasificación de acuerdo con las reglas establecidas en el inciso 7.2.1. Se consideran elementos como informes impresos, pantallas, medios de almacenamiento (cintas, discos, CDs, casetes), mensajes electrónicos y transferencias de archivos.
Para cada nivel de clasificación, los procedimientos de manipulación incluyendo el procesamiento seguro, copia, almacenamiento, transmisión, clasificación y destrucción deben ser definidos.

Los acuerdos con otras organizaciones que compartan información deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.

Otra información

El marcado y la manipulación segura de la información clasificada es un requisito clave para acuerdos de información compartida. Las etiquetas físicas son una forma común de marcado. Sin embargo, algunos activos de información, como documentos electrónicos, no pueden ser físicamente marcados por lo que medios electrónicas para marcar deben ser usadas. Por ejemplo, etiquetas de notificación pueden aparecer en la pantalla. Donde el marcado no se fiable, otras formas de designar la clasificación de la información pueden aparecer.

8. SEGURIDAD EN RECURSOS HUMANOS

8.1 Seguridad antes del empleo1

OBJETIVO: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y que sean adecuados para los roles para los que han sido considerados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.

[1] La palabra empleo hace referencia a cualquiera de las siguientes situaciones: empleo de personal (temporal o de larga duración), reuniones de roles de trabajo, cambio de roles de trabajo, asignación de contratos y la culminación de cualquiera de estos acuerdos.

Las responsabilidades de la seguridad se deben tratar antes del empleo en funciones adecuadas descritas y en términos y condiciones del empleo.

Todos los candidatos para empleo, contratistas y usuarios de terceros deben ser adecuadamente seleccionados, especialmente para trabajos sensibles.

Empleados, contratistas y terceros que utilizan las instalaciones del procesamiento de información deben firmar un acuerdo de confidencialidad.

8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales

Control

Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización.

Guía de implementación

Las funciones de seguridad y las responsabilidades deben incluir los siguientes requisitos:

a) implementadas y realizadas en concordancia con la política de seguridad de la organización (véase el inciso 5.1);

b) deben proteger a los activos de un acceso no autorizado, modificación, destrucción o interferencia;

c) ejecutar procesos particulares o actividades;

d) asegurar que la responsabilidad sea asignada al individuo para tomar acciones;

e) reportar eventos de seguridad o eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones de seguridad y la responsabilidad deben ser definidas y comunicadas claramente a los candidatos al trabajo durante el proceso de selección.

Otra información

Las descripciones de trabajo pueden ser usadas para documentar funciones de seguridad y responsabilidades. Las funciones de seguridad y las responsabilidades para individuos no relacionados con el proceso de selección de la organización, como por ejemplo los que se encuentran comprometidos a través de una organización de terceros, debe ser también claramente definida y comunicada.

8.1.2 Selección y política de personal

Control

Se debe llevar listas de verificación anteriores de todos los candidatos para empleo, contratistas y terceros en concordancia con las leyes , regulaciones y la ética, al igual que proporcionalmente a los requerimientos del negocio, la clasificación de la información ha ser acezada y los riesgos percibidos.

Guía de implementación

Las listas de verificación deben tomar en cuenta la privacidad, la protección de los datos del personal y/o el empleo basado en la legislación y debe permitir incluir lo siguiente:

a) la disponibilidad de referencias satisfactorias sobre actitudes, por ejemplo, una personal y otra de la organización;

b) la comprobación (de los datos completos y precisos) del Curriculum Vitae del candidato;

c) la confirmación de las certificaciones académicas y profesionales;

d) una comprobación independiente de la identificación (con pasaporte o documento similar);

e) comprobaciones mas detalladas, como criminales o de crédito.

La organización debería considerar realizar una comprobación mas detallada a largo plazo de la persona cuando acceda por su empleo, en contratación inicial o en promoción, a recursos de tratamiento de la información y en particular trate información sensible, por ejemplo, información financiera o altamente confidencial.

Los procedimientos deben definir criterios y limitaciones para realizar la verificación, por ejemplo quien es elegible para escoger personas y como, cuando y porque las verificaciones son llevadas a cabo.

Un proceso similar de selección debería realizarse para el personal temporal y subcontratado. Cuando este personal proceda de una agencia el contrato con ésta debería especificar claramente sus responsabilidades en la selección, así como los procedimientos de notificación requeridos si las pruebas de selección no se han completado o si sus resultados son dudosos o preocupantes. De la misma manera, el acuerdo con terceros (véase también 6.2.3) debe especificar claramente todas las responsabilidades y los procedimientos notificados para la selección.

La información de todos los candidatos que han sido considerados para posiciones en la organización deben ser recolectados y maniobrados en concordancia con cualquier legislación apropiada y existente en la jurisdicción relevante. Dependiendo de la legislación aplicable, los candidatos deben ser informados de antemano sobre las actividades de selección.

8.1.3 Acuerdos de confidencialidad

Control

Como parte de su obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Guía de implementación

Los términos y condiciones del empleo deben reflejar la política de organización de la organización además de aclarar y establecer:

a) que todos los empleados, contratistas y terceros a los que se les ha dado acceso a información sensible deben firmar un acuerdo de confidencialidad y de no divulgación antes de darle el acceso a las instalaciones de procesamiento de información;

b) las responsabilidades y derechos del contratista de empleados o cualquier otro usuario, por ejemplo en relación con la legislación de la protección de las leyes o de los datos del derecho del autor;

c) las responsabilidades para la clasificación de la información y la gestión de los activos organizacionales asociados con los sistemas de información y los servicios maniobrados por el empleado, contratista o tercero (véase también 7.2.1 y 10.7.3);

d) las responsabilidades del empleado, contratista o terceros para maniobrar la información recibida de otras compañías o terceros;

e) las responsabilidades de la organización para maniobrar información personal, incluyendo información creada como resultado del empleo en la organización;

f) las responsabilidades que son extendidas fuera de las premisas de la organización y fuera del periodo normal del trabajo, como por ejemplo en el caso del trabajo en casa, (véase también 9.2.5 y 11.7.1);

g) las acciones ha ser tomadas si el empleado, contratista o tercero no cumple con los requisitos de seguridad de la organización (véase también 8.2.3).

La organización debe asegurarse que los empleados, contratistas y usuarios de terceros acepten los términos y condiciones referentes a la seguridad de información apropiada a la naturaleza y al grado de acceso que tendrán con los activos de la organización asociados a los sistemas y a los servicios de información.

Donde sea apropiado, las responsabilidades contenidas en los términos y condiciones del empleo deben continuar por un periodo definido después del termino del este (véase también 8.3).

Otra información

Un código de conducta puede ser usado para cubrir las responsabilidades con respecto a la confidencialidad, protección de datos, ética, uso apropiado del equipo de la organización e instalaciones, así como de empleados, contratistas o terceros, practicas honradas esperadas por la organización. El contratista o tercero puede ser asociado con una organización externa que pueda ser requerida a entrar en acuerdos contractuales a favor del individuo contratado.

8.2 Durante el empleo

OBJETIVO: Asegurar que los empleados, contratistas, y usuarios de terceros estén consientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo y de reducir el riesgo de error humano.

Las responsabilidades de la gerencia deben ser definidas para asegurar que la seguridad sea aplicable a través del empleo de un individuo dentro de la organización.

Un nivel adecuado de conocimiento, educación y entrenamiento en procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información debe ser provista a todos los empleados, contratistas y usuarios de terceros con el fin de minimizar los

posibles riesgos de seguridad. Se debe establecer un proceso disciplinario formal para maniobrar aberturas de seguridad.

8.2.1 Responsabilidades de la gerencia

Control

La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.

Guía de implementación

Las responsabilidades de la gerencia deben incluir, asegurarse de que los empleados, contratistas y terceros:

a) cuenten con un resumen apropiado de sus responsabilidades y roles en la seguridad de información antes de garantizar el acceso a información sensible o a los sistemas de información;

b) que estén provistos con una guía que establezca las expectativas de seguridad de su rol dentro de la organización;

c) que se encuentren motivados de cumplir las políticas de seguridad de la organización;

d) alcancen un nivel de conocimiento de seguridad relevante en sus roles y responsabilidades dentro de la organización (véase el inciso 8.2.2);

e) que estén conforme con los términos y condiciones del empleo, los cuales incluyen la política de seguridad de información de la organización y métodos apropiados de trabajo;

f) continúen teniendo habilidades y calificaciones apropiadas.

Otra información

Si los empleados, contratistas y los usuarios de terceros no están al tanto de sus responsabilidades de seguridad pueden causar daños considerables a al organización. Personal motivado son mas confiables y pueden causar menos incidentes en la seguridad de información.

La mala gestión puede causar al personal sentirse infravalorado resultando en un impacto negativo en la seguridad de la organización. Por ejemplo, puede llevar a que la seguridad sea descuidada o utilizar de forma inadecuada de los activos de la organización.

8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información

Control

Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Guía de implementación

El entrenamiento en el conocimiento debe empezar con una inducción formal del proceso designado para introducir la política de seguridad de la organización y las expectativas, antes conceder acceso a la información o al servicio.

El entrenamiento en curso debe incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como practicas en el uso correcto de los recursos de tratamiento de información (procedimientos de concesión (log-on), uso de paquetes de software e información en el proceso disciplinario (véase el inciso 8.2.3)).

Otra información

El conocimiento sobre seguridad, educación y actividades de entrenamiento deben ser de acuerdo y pertinentes al papel de la persona, las responsabilidades y habilidades deben incluir la información sobre las amenazas conocidas que permitan informar al consejo de seguridad superior a través de los caminos apropiados los eventos relacionados con la seguridad de información (véase el inciso 13.1).

Si se entrena para reforzar el conocimiento, permitirá a los individuos reconocer la seguridad de la información, los problemas y causas, y responder según las necesidades de su papel de trabajo.

8.2.3 Proceso disciplinario

Control

Debe existir un proceso formal disciplinario para empleados que han cometido un apertura en la seguridad.

Guía de implementación

El proceso disciplinario no debe comenzar sin una verificación previa de que la apertura en la seguridad ha ocurrido (véase el inciso 13.2.3).

El proceso formal disciplinario debe asegurar un correcto y justo tratamiento de los empleados que son sospechosos de cometer aperturas en la seguridad. El proceso formal disciplinario debe proveer para una respuesta graduada que tome en consideración factores como la naturaleza, la gravedad de la apertura y su impacto en el negocio, si es que la ofensa es repetida o única o si es que el violador estuvo propiamente entrenado, leyes relevantes, contratos de negocio así como otros factores si son requeridos. En casos serios de mala conducta el proceso debe permitir el retiro de sus labores, derechos de acceso y privilegios así como una escolta inmediata fuera del sitio, si es que es necesario.

Otra información

El proceso disciplinario debe ser usado también como un impedimento para prevenir que los empleados, contratistas y usuarios de terceros violen las políticas y procedimientos organizacionales, así como cualquier otra apertura en la seguridad.

8.3 Finalización o cambio del empleo

OBJETIVO: Asegurar que los empleados, contratistas e usuarios de terceros salgan de la organización o cambien de empleo de una forma ordenada.

Las responsabilidades se establecen con el fin de asegurarse que la salida de la organización de los empleados, contratistas e usuarios de terceros este manejada y que el retorno de todo el equipo y el retiro de todo derecho acceso este completado.

Cambios en la responsabilidad y empleos dentro de la organización deben ser manejados como la terminación de la respectiva responsabilidad o empleo, en línea con esta sección y cualquier nuevo empleo debe ser manejado como se describió en la sección 8.1.

8.3.1 Responsabilidades de finalización

Control

Las responsabilidades para realizar la finalización de un empleo o el cambio de este deben ser claramente definidas y asignadas.

Guía de implementación

La comunicación de la finalización de las responsabilidades deben incluir requisitos de seguridad en curso y responsabilidades legales y donde sea apropiado, responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad (véase el inciso 6.1.5) y términos y condiciones (véase el inciso 8.1.3) continuas por un periodo definido después del termino del contrato de empleo o de terceros.

Las responsabilidades y tareas que son todavía validad después de la finalización del empleo deben ser contenidas en el contrato de empleo o en los contratos de terceros.

Los cambios de responsabilidad o empleo deben ser maniobrados como la finalización de la respectiva responsabilidad o empleo y la nueva responsabilidad o empleo debe ser controlada como se describe en la sección 8.1.

Otra información

La función de recursos humanos es generalmente responsable por la finalización general del proyecto y trabaja conjuntamente con el supervisor de la persona que deja de manejar los aspectos de seguridad de los procedimientos relevantes. En el caso de un contratista, este proceso de la responsabilidad de finalización puede ser tomado en cuenta por una agencia responsable del contratista y en caso sea otro usuario, esto debe ser manejado por la organización.

Puede ser necesario informar a los empleados, clientes, contratistas o terceros los cambios del personal y arreglos de operación.

8.3.2 Retorno de activos

Control

Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.

Guía de implementación

El proceso de finalización debe ser formalizado para incluir el retorno previo de los software, documentos corporativos y equipos. Otros activos de la organización como dispositivos móviles de computo, tarjetas de crédito, tarjetas de acceso, manuales, software e información guardada en medios electrónicos, también necesitan ser devueltos.

En casos donde el empleado, contratista o tercero compra el equipo de la organización o usa su propio equipo, se debe seguir procedimientos para asegurar que toda la información relevante es transferida a la organización y borrado con seguridad del equipo (véase el inciso 10.7.1).

En casos donde un empleado, contratista o tercero tiene conocimiento que es importante para las operaciones en curso, esa información debe ser documentada y transferida a la organización.

8.3.3 Retiro de los derechos de acceso

Control

Los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información deben ser removidos hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio.

Guía de implementación

Hasta la culminación, se debe reconsiderar los derechos de acceso de un individuo a los activos asociados con los sistemas de información y a los servicios. Esto determinara si es necesario retirar los derechos de acceso. Los cambios en un empleo deben ser reflejados en el retiro de todos los derechos de acceso que no fueron aprobados para el nuevo empleo. Los derechos de acceso deben ser removidos o adaptados, incluyendo acceso físico y lógico, llaves, tarjetas de identificación, instalaciones del proceso de información (véase el inciso 11.2.4), subscripciones y retiro de cualquier documentación que los identifica como un miembro actual de la organización. Si un empleado, contratista o usuario de tercero saliente ha sabido contraseñas para activos restantes de las cuentas, deben ser cambiadas hasta la finalización o cambio del empleo, contrato o acuerdo.

Los derechos de acceso para activos de información y equipos de deben ser reducidos o removidos antes que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo como:

a) si la finalización o cambio es iniciado por el empleado, contratista o usuario de tercero, o por la gerencia y la razón de la finalización;

b) las responsabilidades actuales del empleado u otro usuario;

c) el valor de los activos a los que se accede actualmente.

Otra información

En ciertas circunstancias los derechos de acceso pueden ser asignados en base a la disponibilidad hacia mas personas que el empleado, contratista o usuario de tercero saliente. En estas circunstancias, los individuos salientes deben ser removidos de cualquier lista de grupos de acceso y se deben realizar arreglos para advertir a los demás empleados, contratistas y usuarios de terceros involucrados de no compartir esta información con la persona saliente.
En casos de gerencia terminada, contrariedad con los empleados, contratistas o usuarios de terceros pueden llevar a corromper información deliberadamente o a sabotear las instalaciones del procesamiento de información. En casos de renuncia de personal, estos pueden ser tentados a recolectar información para usos futuros.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 Áreas seguras

OBJETIVO: Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias.

Dicha protección debería ser proporcional a los riesgos identificados.

9.1.1 Perímetro de seguridad física

Control

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información e recursos de procesamiento de información.

Guía de implementación

Las siguientes pautas deben ser consideradas e implementadas donde sea apropiado para los perímetros de seguridad físicos.

a) el perímetro de seguridad debería estar claramente definido y el lugar y fuerza de cada perímetro debe depender de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos;

b) el perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física (por ejemplo no tendrá zonas que puedan derribarse fácilmente). Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados, por ejemplo, con mecanismos de control, alarmas, rejas, cierres, etc., las puertas y las ventanas deben ser cerradas con llave cuando estén desatendidas y la protección externa debe ser considerado para ventanas, particularmente al nivel del suelo;

c) se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir sólo al personal autorizado;

d) las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno;

e) todas las puertas para incendios del perímetro de seguridad deberían tener alarma, ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel requerido de resistencia en concordancia con los estándares regionales, nacionales e internacionales apropiados; deben operar en concordancia con el código de fuego local como una forma de seguridad;

f) se debe instalar sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y deben ser regularmente probados para cubrir todas las puertas externas y ventanas de acceso, las áreas no ocupadas deben

tener una alarma todos el tiempo, también se debe cubrir otras áreas como las salas de computo o las salas de comunicación;

g) los recursos de procesamiento de información manejadas por la organización deben ser físicamente separadas de las que son manejadas por terceros.

Otra información

La protección física puede ser lograda creando una o mas barreras físicas alrededor de las premisas de la organización y los recursos de procesamiento de información. El uso de múltiples barreras nos brinda protección adicional, donde la falla de una sola barrera no significa que la seguridad este inmediatamente comprometida.

Un área de seguridad puede ser una oficina cerrada o diversos espacios rodeados por una barrera continua de seguridad interna. Barreras adicionales y perímetros para controlar el acceso físico pueden ser necesarios entre áreas con requisitos de seguridad diferentes dentro del perímetro de seguridad.

Consideraciones especiales hacia la seguridad en el acceso físico deben ser dados a edificios donde existan establecidas organizaciones múltiples.

9.1.2 Controles físicos de entradas

Control

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado.

Guía de implementación

Deberían considerarse las siguientes pautas:

a) las visitas a las áreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha y momento de entrada y salida. Los visitantes sólo tendrán acceso para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia;

b) se debería controlar y restringir sólo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento. Se deberían usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso. Se debería mantener un rastro auditable de todos los accesos, con las debidas medidas de seguridad;

c) se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique;

d) se debe garantizar el acceso restringido al personal de apoyo de terceros, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este sea requerido. Este acceso debe ser autorizado y monitoreado;

e) se deberían revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad (véase el inciso 8.3.3).

9.1.3 Seguridad de oficinas, despachos y recursos

Control

La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada.

Guía de implementación

Las siguientes pautas deberían ser consideradas:

a) se debería tomar en cuenta las regulaciones y estándares de salud y seguridad;

b) se deben instalar equipos con clave deben para evitar el acceso del publico;

c) donde sea aplicable, los edificios deben ser discretos y dar una mínima indicación de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información;

d) los directorios y las guías telefónicas internas identificando locaciones de los recursos de información sensible no deben ser fácilmente accesibles por el publico.

9.1.4 Protección contra amenazas externas y ambientales

Control

Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.

Guía de implementación

Se debe dar consideración a cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.

Las siguientes pautas deben ser consideradas para evitar daño por parte del fuego, inundación, temblores, explosiones, malestar civil y otras formas de desastre natural o humana:

a) los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante de las áreas seguras. No se deberían almacenar dentro de un área segura suministros a granel hasta que se necesiten;

b) el equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal;

c) equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente.

9.1.5 El trabajo en las áreas seguras

Control

Se debería diseñar y aplicar protección física y pautas para trabajar en áreas seguras.

Guía de Implementación

Se deben considerar las siguientes pautas:

a) el personal sólo debería conocer la existencia de un área segura, o de sus actividades, si lo necesitara para su trabajo;

b) se debería evitar el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas;

c) las áreas seguras deberían estar cerradas y controlarse periódicamente cuando estén vacías;

d) no se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial;

Los arreglos para trabajar en áreas seguras deben incluir controles para los empleados, contratistas y usuarios de terceros que trabajen en dicha área, así como otras actividades de terceros que se lleven acabo ahí.

9.1.6 Acceso publico, áreas de carga y descarga

Control

Se deberían controlar las áreas de carga y descarga, y si es posible, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.

Guía de implementación

Se deben considerar las siguientes pautas:

a) se deberían restringir los accesos al área de carga y descarga desde el exterior únicamente al personal autorizado e identificado;

b) el área de carga y descarga se debería diseñar para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio;

c) la puerta externa del área debería estar cerrada cuando la interna esté abierta;

d) el material entrante se debería inspeccionar para evitar posibles amenazas segregado (véase el inciso 9.2.ld) antes de llevarlo a su lugar de utilización;

e) el material entrante se debería registrar en concordancia con los procedimientos de gestión de activos (véase el inciso 7.1.1*)* al entrar en el lugar;

f) el material entrante y saliente debería ser físicamente separado, donde sea posible.

9.2 Seguridad de los equipos

OBJETIVO: Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

El equipo debería estar físicamente protegido de las amenazas.

También se debería considerar su instalación (incluyendo su uso fuera del local) y disponibilidad. Pueden requerirse medidas o controles especiales contra riesgos de accesos no autorizados y para proteger los sistemas de apoyo, como la alimentación interrumpida o la infraestructura de cableado.

9.2.1 Instalación y protección de equipos

Control

El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.

Guía de implementación

Se deberían considerar los siguientes pautas para proteger los equipos:

a) los equipos se deberían situar dónde se minimicen los accesos innecesarios a las áreas de trabajo;

b) los equipos de tratamiento y almacenamiento de información que manejen datos sensibles se deberían instalar dónde se reduzca el riesgo de que personas no autorizadas vean los procesos durante su uso;

c) los elementos que requieran especial protección se deberían aislar para reducir el nivel general de protección requerido;

d) los controles deben ser adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo;

e) la organización debería incluir en su política cuestiones sobre fumar, beber y comer cerca de los equipos de tratamiento de información;

f) se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información;

g) la protección contra la luz debe ser aplicada a todos los edificios y se deben ajustar filtros de luz a todas las líneas de poder y de comunicación;

h) para los equipos situados en ambientes industriales se debería considerar el uso de métodos de protección especial (por ejemplo cubiertas para teclados);

i) el equipo que procesa información sensible debe ser protegida con el fin de minimizar el riesgo de perdidas de información.

9.2.2 Suministro eléctrico

Control

Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.

Guía de implementación

Todos las instalaciones de apoyo, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado debe ser adecuado para los sistemas que están apoyando. Los equipos de apoyo deben ser inspeccionados regularmente y probados apropiadamente para asegurar su funcionamiento apropiado y para reducir cualquier riesgo causado por su mal funcionamiento o por una falla. Un suministro eléctrico adecuado debe ser provisto que sea conforme con las especificaciones del fabricante del equipo.

Se recomienda instalar un Sistema de Alimentación Ininterrumpida (U.P.S.) para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio. Se deberían cubrir mediante planes de contingencia las acciones a adoptar en caso de fallo del UPS. Si el proceso debería continuar en caso de fallo prolongado de energía se debería instalar un generador de respaldo. En este caso, se debería probar regularmente de acuerdo con las recomendaciones del fabricante. Se debería disponer de una reserva suficiente de combustible para asegurar el funcionamiento del generador durante un periodo prolongado.
Los equipos de UPS y los generadores se deberían revisar regularmente para asegurar que tienen la capacidad adecuada y que están probados de acuerdo con las recomendaciones del fabricante. En adición, se pueden dar consideraciones para el uso de múltiples fuentes de poder o si el lugar es amplio, una subestación de poder separada.

Además se deberían instalar interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se debería disponer de alumbrado de emergencia.

El suministro de agua debe ser estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados). Problemas con el suministro de agua pueden dañar el equipo o hacer que los sistemas contra incendios no funcionen efectivamente. Un sistema de alarma para detectar problemas de funcionamiento en las instalaciones de apoyo debe ser evaluado e instalado si es requerido.

Los equipos de telecomunicación deben ser conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio debe ser adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.

Otra información

Las opciones para lograr continuidad en el suministro de energía incluyen alimentación múltiple con el fin de evitar un punto simple de falla.

9.2.3 Seguridad del cableado

Control

Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.

Guía de implementación

Se deberían considerar los siguientes pautas para la seguridad del cableado:

a) las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, se deberían enterrar, cuando sea posible, o adoptarse medidas alternativas de protección;

b) la red cableada se debería proteger contra intercepciones no autorizadas o daños, por ejemplo, usando conductos y evitando rutas a través de áreas públicas;

c) se deberían separar los cables de energía de los de comunicaciones para evitar interferencias;

d) cables claramente identificados y marcas de equipo deben ser utilizadas con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta;

e) un lista documentada de parches debe utilizarse con el fin de reducir la posibilidad de errores;

f) se deberían considerar medidas adicionales para sistemas sensibles o críticos, como:

1) instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación;

2) uso de rutas o de medios de transmisión alternativos;

3) uso de cableado de fibra óptica;

4) uso de un escudo electromagnético para proteger los cables;

5) inicialización de inspecciones físicas y técnicas a los dispositivos no autorizados adjuntados a los cables;

6) acceso controlado para parchar paneles y cuartos de cable.

9.2.4 Mantenimiento de equipos

Control

Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

Guía de implementación

Las siguientes pautas para el mantenimiento de los equipos deberían ser considerados:

a) los equipos se deberían mantener de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador;

b) sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos;

c) se deberían registrar documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo;

d) se debería implementar controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal

interno o externo a la organización; donde sea necesario, debe despejarse la información sensible del equipo;

e) se deberían cumplir todos los requisitos impuestos por las políticas de los seguros.

9.2.5 Seguridad de equipos fuera de los locales de la organización

Control

Se debe aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización tomando en cuenta los diversos riesgos a los que se esta expuesto.

Guía de implementación

Sólo la gerencia debería poder autorizar el uso de cualquier equipo para tratamiento de información fuera de los locales de la organización, sea quien sea su propietario.

a) los equipos y medios que contengan datos con información y sean sacados de su entorno habitual no se deberían dejar desatendidos en sitios públicos. Cuando viajen, los computadores portátiles se deberían transportar de una manera disimulada como equipaje de mano;

b) se deberían observar siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos;

c) los controles para el trabajo en el domicilio se deberían determinar mediante una evaluación de los riesgos y aplicarse los controles convenientes según sea apropiado, por ejemplo, en controles de acceso a los computadores, una política de puesto de trabajo despejado y cierre de las zonas de archivo (véase también ISO/IEC 18028 Seguridad de Redes.);

d) se deberían cubrir con un seguro adecuado los equipos fuera de su lugar de trabajo.

Los riesgos de seguridad, por ejemplo, de daño, robo y escucha, pueden variar mucho según la ubicación y ésta debería tenerse en cuenta al determinar los controles más apropiados.

Otra información

Los equipos de almacenamiento y procesamiento de información incluyen todas las formas de computadores personales, organizadores, teléfonos celulares, tarjetas inteligentes, papel u otra forma que se utilice para trabajo en el domicilio o que pueda ser transportado fuera del lugar normal de trabajo.

Puede encontrarse en el inciso 11.7.1 más información sobre otros aspectos de la protección de equipos móviles.

9.2.6 Seguridad en el rehúso o eliminación de equipos

Control

Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.

Guía de implementación

Los dispositivos de almacenamiento con información sensible se deberían destruir físicamente o la información debe ser destruida, borrada o sobrescrita usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.

Otra información

Los dispositivos dañados que contienen data sensible pueden requerir una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.

La información puede ser comprometida a través de dispositivos descuidados o por el re uso del equipo (véase el inciso 10.7.2).

9.2.7 Retiro de la propiedad

Control

El equipo, información o software no debe ser sacado fuera del local sin autorización.

Guía de implementación

Se deben de considerar las siguientes pautas:

a) el equipo, información o software no debe ser sacado fuera del local sin autorización;

b) los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos deben ser claramente identificados;

c) los tiempos limite para el retiro de equipos deben ser fijados y el retorno del equipo verificado para asegurar la conformidad;

d) el equipo debe ser registrado, si es necesario y apropiado, cuando este sea removido fuera del local así como cuando sea devuelto.

Otra información

También pueden realizarse notas de salida, emitidos para descubrir si existen salidas desautorizadas de la propiedad, para descubrir dispositivos magnetofónicos desautorizado, armas, etc., y previene su entrada en el lugar. Las notas de salida deben llevarse a cabo siguiendo la legislación pertinente y las regulaciones. Los individuos deben ser conscientes de que estos documentos se emiten solo con la autorización apropiada y los requisitos legales y reguladores.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Procedimientos y responsabilidades de operación

OBJETIVO: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

10.1.1 Documentación de procedimientos operativos

Control

Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.

Guía de implementación

Se debe preparar los procedimientos documentados para actividades del sistema asociados con el procesamiento de información y los recursos de comunicación, como los procedimientos de prendido y apagado de la computadora, backups, mantenimiento de equipos, manipulación de medios, ambientes de computo y manipulación de correos, y seguridad.

Dichos procedimientos deberían especificar las instrucciones necesarias para la ejecución detallada de cada tarea, incluyendo:

a) el proceso y utilización correcto de la información;

b) backup (véase el inciso 10.5);

c) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos de comienzo más temprano y final más tardío posibles de cada tarea;

d) las instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la tarea de ejecución, incluyendo restricciones en el uso de servicios del sistema (véase el inciso 11.5.4);

e) los contactos de apoyo en caso de dificultades inesperadas operacionales o técnicas;

f) las instrucciones especiales de utilización de resultados, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de destrucción segura de resultados producidos como consecuencia de tareas fallidas (véase también 10.7.2 y 10.7.3);

g) el reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema;

h) la gestión de la información del rastro de auditoria y del registro de sistema (véase el inciso 10.10).

Se deberían preparar procedimientos documentados para las actividades de administración del sistema y cualquier cambio que se deba realizar debe ser autorizado por la gerencia. Donde sea técnicamente viable, los sistemas de información deben ser gestionados consistentemente usando los mismos procedimientos, herramientas y recursos.

10.1.2 Gestión de Cambios

Control

Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información.

Guía de Implementación

Los sistemas operacionales y los software de aplicación deben ser sujetos a un estricto control de la gestión de cambios.

En particular se deberían considerar los siguientes controles y medidas:

a) la identificación y registro de cambios significativos;

b) planeamiento y prueba de los cambios;

c) la evaluación de los posibles impactos, incluyendo impactos de seguridad, de dichos cambios;

d) un procedimiento formal de aprobación de los cambios propuestos;

e) la comunicación de los detalles de cambio a todas las personas que corresponda;

f) procedimientos que identifiquen las responsabilidades de abortar y recobrarse de los cambios sin éxito y de acontecimientos imprevistos.

Se deberían implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se cambien los programas se debería conservar un registro de auditoria conteniendo toda la información importante.

Otra información

El control inadecuado de los cambios a los sistemas y recursos de procesamiento de información es una causa común de fallas del sistema o de seguridad. Cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la de operación, pueden impactar en la fidelidad de las aplicaciones (véase el inciso 12.5.1).

Los cambios a los sistemas operacionales deben realizarse solamente cuando existe una razón de negocio valida, como un incremento en el riesgo al sistema. Actualizando los sistemas con la ultima versión de los sistemas operativos o aplicaciones, no siempre se encuentra en los intereses del negocio además de que puede introducir mayores vulnerabilidades e inestabilidad que la versión actual. También se puede necesitar de un entrenamiento adicional, costos de licencias, apoyo, mantenimiento y administración, y un nuevo hardware especialmente durante la migración.

10.1.3 Segregación de tareas

Control

Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización.

Guía de implementación

La segregación de tareas es un método para reducir el riesgo de mal uso accidental o deliberado de un sistema. Se debe tener cuidado de que cualquier persona puede acceder, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento debe estar separado de su autorización. La posibilidad de confabulación debe ser considerada en el diseño de los controles.

Las organizaciones pequeñas pueden considerar que este método de control es difícil de lograr, pero el principio debería aplicarse en la medida en que sea posible y practicable. Cuando la segregación sea difícil, se considerarán otros controles como la monitorización de las actividades, las pistas de auditoria y la supervisión de la gestión. Es importante que la auditoria de seguridad permanezca independiente.

10.1.4 Separación de los recursos para desarrollo y para producción

Control

La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

Guía de Implementación

Se debería identificar e implementar controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción que es necesario para evitar problemas operacionales.

Se debería considerar lo siguiente:

a) las reglas de transferencia del software desde un estado de desarrollo al de producción deben ser definidos y documentados;

b) el software de desarrollo y el de producción deberían, si es posible, funcionar en procesadores diferentes, o en dominios o directorios distintos;

c) los compiladores, editores y otros servicios del sistema no deberían ser accesibles desde los sistemas de producción, cuando no se necesiten;

d) el entorno de prueba del sistema debe emular el entorno del sistema operacional lo mas cercano posible;

e) los usuarios deben utilizar diferentes perfiles de usuario para los sistemas operacionales y de prueba; y los menús deben exhibir mensajes de identificación apropiados con el fin de reducir el riesgo por error;

f) los datos sensibles no deben ser copiados en el entorno del sistema de prueba.

Otra Información

Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo, cambios no deseados en los archivos o en el entorno del sistema o fallos del sistema. En este caso es necesario mantener un entorno conocido y estable para poder realizar las pruebas significativas y evitar el acceso inapropiado del personal de desarrollo.
Si el personal de desarrollo y el de prueba tuvieran acceso al sistema de producción y a su información, podrían introducir un código no autorizado o no probado o alterar los datos operacionales. En algunos sistemas esta posibilidad podría utilizarse de forma indebida, para

cometer fraudes o para introducir un código no probado o malicioso, lo que podría causar problemas operacionales serios.

Los encargados del desarrollo o de las pruebas también suponen una amenaza a la confidencialidad de la información de producción. Las actividades de desarrollo y de prueba pueden causar cambios inesperados en el software y la información si comparten el mismo entorno de tratamiento. La segregación de los recursos de desarrollo, prueba y producción es conveniente para reducir el riesgo de cambios accidentales o del acceso no autorizado al software de producción y a los datos de la organización (véase el inciso 12.4.2 para la protección de los datos de prueba).

10.2 Gestión de servicios externos

OBJETIVO: Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros.

La organización debe verificar la implementación de acuerdos, el monitoreo de la conformidad con los acuerdos y los cambios gestionados con el fin de asegurar que todos los servicios entregados cumplen con todos los requerimientos acordados con terceros.

10.2.1 Servicio de entrega

Control

Debemos asegurarnos que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluidas en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.

Guía de Implementación

El servicio entregado por terceros debe incluir los arreglos de seguridad acordados, definiciones de servicio y aspectos de la gestión del servicio. En caso de arreglos de outsourcing, la organización debe planear las transiciones (de información, recursos del procesamiento de información y cualquier otra cosa que requiere ser movido), y debe asegurar que la seguridad sea mantenida a través del periodo de transición.

La organización debe asegurarse que los terceros mantengan una capacidad suficiente junto con planes realizables designados para asegurar que los niveles continuos del servicio acordado sean mantenidos siguiendo fallas mayores del servicio o desastre (véase 14.1).

10.2.2 Monitoreo y revisión de los servicios externos

Control

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorias deben ser llevadas a cabo regularmente.

Guía de Implementación

El monitoreo y la revisión de los servicios externos debe asegurarse que todos los términos de seguridad de la información y las condiciones de los acuerdos han sido adheridos, y que los incidentes y problemas en la seguridad de información han sido manejados propiamente. Esto debe implicar una relación y proceso de gestión del servicio entre la organización y terceros para:

a) servicio de monitoreo de niveles de funcionamiento para verificar que se adhieran a los acuerdos;

b) reportes de revisión de servicio producidos por terceros y que arregle reuniones regulares de progreso como requieran los acuerdos;

c) proveer información acerca de los incidentes de seguridad de información y revisión de esta información por terceros y la organización como requiera los acuerdos y cualquier pautas de apoyo y procedimientos;

d) revisar los acuerdos y los rastros de intervención de los eventos de seguridad, problemas operacionales, fallas, trazabilidad de faltas e interrupciones relacionadas con el servicio entregado;

e) resolver y manejar cualquier problema identificado.

La responsabilidad para manejar las relaciones con un tercero debe ser asignado a un individuo designado o a un equipo de gestión de servicio. La organización debe asegurar que los proveedores externos asignen responsabilidades para verificar la conformidad y el cumplimiento de los requisitos de los acuerdos. Deben estar disponibles habilidades y recursos suficientes para monitorear los requisitos de los acuerdos (véase 6.2.3), en particular los requisitos de seguridad de información. Se deben de tomar acciones apropiadas cuando se observen deficiencias en el servicio entregado.

La organización debe mantener un control y una visión general suficiente en todos los aspectos para información sensible o critica o a los recursos del procesamiento de información accedidos, procesados o gestionados por terceros. La organización debe asegurar que retengan la visión en las actividades de seguridad como el cambio en la gerencia, identificación de las vulnerabilidades e incidentes de la seguridad de información.

Otra información

En caso de outsourcing, la organización necesita estar al tanto que la ultima responsabilidad para el procesamiento de información realizada por un tercero recae en la organización.

10.2.3 Gestionando cambios para los servicios externos

Control

Cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes.

Guía de Implementación

El proceso de gestionar cambios para los servicios externos necesita tomar en cuenta lo siguiente:

a) cambios realizados por la organización para implementar:

1) realces en el actual servicio ofrecido;

2) desarrollo de cualquier aplicación o sistema nuevo;

3) modificaciones o actualizaciones de las políticas y procedimientos organizacionales;

4) controles nuevos para resolver incidentes en la seguridad de información y para mejorar la seguridad;

b) cambios en los servicios externos para implementar:

1) cambios y realces en las redes;

2) el uso de nuevas tecnologías;

3) adopción de nuevos productos o versiones o lanzamientos nuevos;

4) nuevas herramientas y ambientes de desarrollo;

5) cambios en la locación física de los recursos de servicio;

6) cambios en el vendedor.

10.3 Planificación y aceptación del sistema

OBJETIVO: Minimizar el riesgo de fallos de los sistemas.

Son necesarios una planificación y preparación para asegurar la disponibilidad de capacidad y de recursos adecuados para entregar el sistema de funcionamiento requerido.

Deberían realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema.

Se debería establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos.

10.3.1 Planificación de la capacidad

Control

El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido.

Guía de control

Para cada actividad que se este llevando a cabo o para una actividad nueva, los requisitos de capacidad deben ser identificados. Se debe aplicar el monitoreo de los sistemas con el fin de asegurar, y donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Controles de detección deben ser instalados pata detectar los problemas en un tiempo debido.
Las proyecciones deberían tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en la organización.

Se requiere poner particular atención a cualquier recurso con tiempo de llegada largo o con costos altos; por esto, la gerencia debe monitorear la utilización de los recursos claves del sistema. Se deberían identificar las tendencias de uso, particularmente relativas a las aplicaciones del negocio o a las herramientas de administración de sistemas de información.

Los administradores deberían usar esta información para identificar y evitar los posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios al usuario, y para planificar la acción correctora apropiada.

10.3.2 Aceptación del sistema

Control

Se deberían establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deberían desarrollar con ellos las pruebas adecuadas antes de su aceptación.

Guía de Implementación

Los administradores se deberían asegurar que los requisitos y criterios de aceptación de los nuevos sistemas estén claramente definidos, acordados, documentados y probados. Los nuevos sistemas de información, actualizaciones y las nuevas versiones deben ser migradas a producción solamente después de obtener una aceptación formal. Se deberían considerar los siguientes puntos antes de obtener la aceptación formal:

a) los requisitos de rendimiento y capacidad de los computadores;

b) los procedimientos de recuperación de errores y reinicio, así como los planes de contingencia;

c) la preparación y prueba de procedimientos operativos de rutina según las normas definidas;

d) un conjunto acordado de controles y medidas de seguridad instalados;

e) manual de procedimiento eficaz;

f) plan de continuidad del negocio como se requiere en el inciso 11.1;

g) la evidencia de que la instalación del nuevo sistema no producirá repercusiones negativas sobre los existentes, particularmente en los tiempos con pico de proceso como a fin de mes;

h) la evidencia de que se ha tenido en cuenta el efecto que tendrá el nuevo sistema en la seguridad global de la organización;

i) la formación en la producción o utilización de los sistemas nuevos.

j) la facilidad de empleo, como este afecta el funcionamiento del usuario y evita los errores humanos.

Para nuevos desarrollos importantes, se debería consultar al responsable de operaciones y a los usuarios en todos los niveles del proceso de desarrollo para asegurar la eficacia operacional del diseño del sistema propuesto. Se deberían realizar pruebas apropiadas para confirmar que se han satisfecho completamente todos los criterios de aceptación.

Otra información

La aceptación puede incluir una certificación formal y un proceso de acreditación para verificar que los requisitos de seguridad han sido apropiadamente anexados.

10.4 Protección contra software malicioso

OBJETIVO: Proteger la integridad del software y de la información.

Se requieren ciertas precauciones para prevenir y detectar la introducción de software malicioso.

El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, “gusanos de la red”, “caballos de troya” y “bombas lógicas”. Los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.

10.4.1 Medidas y controles contra software malicioso

Control

Se deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.

Guía de Implementación

La protección contra el software malicioso debería basarse en la conciencia de la seguridad, en sistemas adecuados de acceso y en controles de gestión de los cambios. Los controles siguientes deberían ser considerados:

a) una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado (véase el inciso 15.1.2);

b) una política formal de protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indicando las medidas protectoras a adoptar;

c) la realización de revisiones regulares del software y de los datos contenidos en los sistemas que soportan procesos críticos de la organización. Se debería investigar formalmente la presencia de todo archivo no aprobado o toda modificación no autorizada;

d) la instalación y actualización frecuente de software de detección y reparación de virus, que exploren los computadores y los medios de forma rutinaria o como un control preventivo; las revisiones llevadas a cabo deben incluir:

1) verificación de archivos electrónicos de origen incierto o no autorizado, o recibidos a través redes no fiables, para comprobar la existencia de virus antes de usarlos;

2) verificación de todo archivo adjunto a un correo electrónico o de toda descarga para buscar software malicioso antes de usarlo. Esta comprobación se hará en distintos lugares, por ejemplo, en los servidores de correo, en los computadores personales o a la entrada en la red de la organización;

3) la verificación de códigos maliciosos en las paginas Web.

e) los procedimientos y responsabilidades de administración para la utilización de la protección de antivirus, la formación para su uso, la información de los ataques de los virus y la recuperación de éstos (véanse los incisos 13.1 y 13.2);

f) los planes de continuidad del negocio apropiados para recuperarse de los ataques de virus, incluyendo todos los datos y software necesarios de respaldo y las disposiciones para la recuperación (véase el capítulo 14);

g) la implementación de procedimientos para recolectar información regularmente, como suscribirse a listas de correo y/o verificar paginas Web que contengan información sobre nuevos virus.

h) los procedimientos para verificar toda la información relativa al software malicioso y asegurarse que los boletines de alerta son precisos e informativos. Los administradores se deberían asegurar que se diferencian los virus reales de los falsos

avisos de virus, usando fuentes calificadas, por ejemplo, revistas reputadas, sitios de Internet fiables o los proveedores de software antivirus. Se debería advertir al personal sobre el problema de los falsos avisos de virus y qué hacer en caso de recibirlos.

Otra información

El uso de dos o mas productos de software protegiéndonos contra códigos maliciosos a través del ambiente de procesamiento de información desde diferentes vendedores puede mejorar la efectividad de esta protección.

Los software que protegen contra códigos maliciosos pueden ser instalados para proveer actualizaciones automáticas de archivos de definición y para explorar los motores para asegurar que la protección se encuentre actualizada. En adición, este software puede ser instalado en cualquier escritorio para llevar a cabo verificaciones automáticas.

Se debe tener mucho cuidado al proteger contra la introducción de código malicioso durante el mantenimiento y los procedimientos de emergencia, ya que estos pueden pasar controles normales de protección.

10.4.2 Medidas y controles contra código móvil

Control

Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado.

Guía de Implementación

Las siguientes acciones deben ser consideradas para protegernos contra acciones no autorizadas de códigos móviles:

a) ejecutar un código móvil en un ambiente lógico aislado;

b) bloquear cualquier uso de código móvil;
c) bloquear el recibo de código móvil;

d) activar medidas técnicas como estén disponibles en un sistema especifico para asegurar que el código móvil esta manejado;

e) controlar los recursos disponibles al acceso de código móvil;

f) controlar criptográficamente para autentificar individualmente un código móvil.

Otra Información

El código móvil es un código de software que se transfiere desde una computadora a otra y luego ejecuta automáticamente y realiza una función especifica con poco o ninguna interacción del usuario. El código móvil esta asociado con un número de servicios middleware.

En adición para asegurar que los códigos móviles no contienen código malicioso, es esencial controlarlos con el fin de evitar un uso desautorizado o una interrupción del sistema, red o aplicaciones y otras ramas de la seguridad de información.

10.5 Gestión de respaldo y recuperación

OBJETIVO: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo (véase el inciso 14.1) haciendo copias de seguridad y ensayando su oportuna recuperación.

10.5.1 Recuperación de la información

Control

Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.

Guía de Implementación

Adecuados servicios de respaldo deben ser provistos para asegurar que toda la información esencial del negocio pueda recuperarse tras un desastre o un fallo de los medios.

Los siguientes puntos de la recuperación de información deben ser considerados:

a) se debería definir el nivel necesario de recuperación de la información;

b) se debería almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación;

c) la extensión y frecuencia de los respaldos deben reflejar las necesidades de la organización, los requisitos de seguridad de la información envuelta, y la criticidad de la información para la operación continua de la organización;

d) los respaldos deben estar almacenados en una locación remota, en una distancia suficiente para escapar de cualquier daño frente a un desastre en el local principal;

e) se debería dar a la información de respaldo un nivel adecuado de protección física y del entorno (véase el capítulo 9), un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo;

f) los medios de respaldo se deberían probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia;

g) se deberían comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación;

h) en situaciones donde la confidencialidad sea importante, los respaldos deben ser protegidos por medios de encriptación.

Deben probarse regularmente arreglos individuales de las copias de seguridad de los sistemas para asegurar que estos reúnen los requisitos de los planes de continuidad del negocio (véase el capitulo 14). Para los sistemas críticos, los arreglos auxiliares deben cubrir toda la información de los sistemas, aplicaciones y datos necesarios de recuperarse del sistema completo en caso de un desastre.

El periodo de retención para la información esencial del negocio, y también cualquier requisito permanente para las copias de los archivos debe determinarse (véanse el inciso 15.1.3).

Otra información

Las copias de seguridad pueden automatizarse para aliviar el proceso de restauración. Deben probarse tales soluciones automatizadas suficientemente antes de la implementación y a intervalos regulares.

10.6 Gestión de seguridad en redes

OBJETIVO: Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

La gestión de la seguridad de las redes que cruzan las fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

Controles adicionales pueden ser requeridos también con el fin de proteger información sensible pasando sobre redes publicas.

10.6.1 Controles de red

Control

Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en transito.

Guía de Implementación

Los administradores de redes deberían implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadores, así como la protección de los servicios conectados contra accesos no autorizados. En particular, se deberían considerar los controles y medidas siguientes:

a) La responsabilidad operativa de las redes debería estar separada de la operación de los computadores si es necesario (véase el inciso 10.1.3);

b) Se deberían establecer responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios;

c) Se deberían establecer, si procede, controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados (véanse los incisos 11.4 y

12.3). También se deberían requerir controles y medidas especiales para mantener la disponibilidad de los servicios de las redes y de los computadores conectados;

d) Un registro y monitoreo apropiado debe ser aplicado para permitir el registro de acciones relevantes de seguridad;

e) Se deberían coordinar estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información.

Otra Información

Información adicional en seguridad de redes puede ser encontrada en ISO/IEC 18028.

10.6.2 Seguridad en los servicios de redes

Control

Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización.

Guía de Implementación

La habilidad del proveedor del servicio de red para manejar servicios acordados de una manera segura debe ser determinado y monitoreado regularmente, y el derecho para auditar debe ser acordado.

Los acuerdos de seguridad necesarios para servicios particulares, como características de seguridad, niveles de servicio y los requisitos de gestión, deben ser identificados. La organización debe asegurarse que los proveedores del servicio de red implementen estas medidas.

Otra información

Los servicios de red incluyen la provisión de conexiones, servicios de red privados y redes de valor agregado así como soluciones manejadas de seguridad de redes como firewalls y sistemas de detección de intrusos. Estos servicios pueden alcanzar desde un simple ancho de bando no manejado hasta ofertas complejas de valor agregado.

Las características de los servicios de seguridad de redes pueden ser:

a) tecnología aplicada para servicios de seguridad de red, como autentificación, encriptado y controles de conexión de red;

b) parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red;

c) procedimientos para el uso de los servicios de red para restringir el acceso a estos servicios o aplicaciones donde sea necesario.

10.7 Utilización de los medios de información

OBJETIVO: Prevenir acceso no autorizado, modificaciones, evitar daños a los activos e interrupciones de las actividades de la organización.

Los medios deben ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado.

10.7.1 Gestión de medios removibles

Control

Debería haber procedimientos para la gestión de los medios informáticos removibles.

Guía de Implementación

Se deberían considerar las siguientes pautas para la gestión de los medios removibles:

a) se deberían borrar cuando no se necesiten más, los contenidos previos de todo medio reutilizable del que se desprenda la organización;

b) donde sea necesario y practico, todo medio desechado por la organización debería requerir autorización y se debería guardar registro de dicha remoción para guardar una pista de auditoria;

c) todos los medios se deberían almacenar a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes;

d) la información almacenada en el medio, que requiere estar disponible mayor tiempo que el tiempo de vida del medio (en concordancia con las especificaciones del productor) debe ser también almacenada con el fin de no perder dicha información debido al deterioro del medio;

e) el registro de los medios removibles debe ser considerado para limitar la oportunidad de perdida de datos;

f) los medios removibles deben ser solo activados si existe una razón de negocio para hacerlo.

Se deberían documentar claramente todos los procedimientos y niveles de autorización.

Otra Información

Los medios removibles incluyen cintas, discos, CDs, DVDs y medios imprimibles.

10.7.2 Eliminación de medios

Control

Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.

Guía de Implementación

Se deberían establecer procedimientos formales para minimizar el riesgo de filtro de información sensible a personas externas con la eliminación segura de los medios. Los procedimientos para la seguridad de los medios que contienen información sensible deben ser conmensurados con la sensibilidad de dicha información. Se deberían considerar los siguientes puntos:

a) los medios que contengan información sensible se almacenarán y eliminarán de forma segura, por ejemplo, incinerándolos, triturándolos o vaciando sus datos para usarlos en otra aplicación dentro de la organización;

b) los procedimientos deben permitir identificar los ítems que puedan requerir un dispositivo de seguridad;

c) puede ser más fácil recoger y eliminar con seguridad todos los tipos de medios que intentar separar los que contienen información sensible;

d) muchas organizaciones ofrecen servicios de recojo y eliminación de papel, equipos y medios. Debería cuidarse la selección de los proveedores adecuados según su experiencia y lo satisfactorio de los controles que adopten;

e) se debería registrar la eliminación de elementos sensibles donde sea posible para mantener una pista de auditoria.

Se debería considerar el efecto de acumulación de medios a la hora de eliminar, ya que puede suceder que una gran cantidad de información no clasificada sea más sensible que una pequeña cantidad de información clasificada.

Otra Información

La información sensible puede ser divulgada a través de medios desechados sin cuidado (véase el inciso 9.2.6).

10.7.3 Procedimientos de manipulación de la información

Control

Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados.

Guía de Implementación

Se deberían establecer procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación (véase el inciso 7.2). Los siguientes ítems deben ser considerados:

a) etiquetado en la administración de todos los medios;

b) restricciones de acceso para identificar al personal no autorizado;

c) mantenimiento de un registro formal de recipientes autorizados de datos;

d) aseguramiento de que los datos de entrada, su proceso y la validación de la salida están completos;

e) protección de los datos que están en cola para su salida en un nivel coherente con su criticidad;

f) almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante;

g) minimizar la distribución de datos;

h) identificación clara de todas las copias de datos para su atención por el receptor autorizado;

i) revisión de las listas de distribución y de receptores autorizados a intervalos regulares.

Otra Información

Estos procedimientos aplican a la información en documentos, sistemas de computo, redes, computadores móviles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios y recursos postales, uso de maquinas de fax y cualquier otro ítem sensible, como cheques o facturas.

10.7.4 Seguridad de la documentación de sistemas

Control

Los documentación de sistemas debe ser protegida contra acceso no autorizado.

Guía de Implementación

Para proteger la documentación de sistemas de accesos no autorizados se deberían considerar lo siguiente:

a) la documentación de sistemas se debería almacenar con seguridad;

b) la lista de acceso a la documentación de sistemas se debería limitar al máximo, y ser autorizada por el propietario de la aplicación;

c) la documentación de sistemas mantenida en una red pública, o suministrada vía una red pública, se debería proteger adecuadamente.

Otra Información

La documentación de sistemas puede contener un rango de información sensible como por ejemplo descripciones de los procesos de las aplicaciones, procedimientos, estructura de datos y autorización de procesos.

10.8 Intercambio de información

OBJETIVO: Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones

Se deberían realizar los intercambios sobre la base de acuerdos formales. Se deberían controlar los intercambios de información y software entre organizaciones, que deberían cumplir con toda la legislación correspondiente (véase el capítulo 15).

Se deberían establecer procedimientos y normas para proteger la información de los medios en tránsito.

10.8.1 Políticas y procedimientos para el intercambio de información y software

Control

Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.

Guía de Implementación

Los procedimientos y controles ha ser seguidos cuando se utilice instalaciones electrónicas de comunicación para el intercambio de información deben considerar lo siguiente:

a) los procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción;

b) los procedimientos para la detección y protección contra código malicioso que puede ser transmitido a través del uso de comunicación electrónica (véase el inciso 10.4.1);

c) los procedimientos para proteger información electrónica sensible que esta en forma de archivo adjunto;

d) las políticas o pautas para el uso aceptable de las instalaciones de comunicación electrónica (véase el inciso 7.1.3);

e) los procedimientos para el uso de comunicaciones inalámbricas, tomando en cuenta los riesgos particulares envueltos;

f) las responsabilidades de los empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por difamación, hostigamiento, personificación, reenvío de cadenas de correos, compra no autorizada, etc;

g) el uso de técnicas criptográficas como por ejemplo para proteger la confidencialidad, integridad y autenticidad de la información (véase el inciso 12.3);

h) las pautas de disposición y retención para toda la correspondencia de negocios, incluyendo mensajes, en concordancia con la legislación y las regulaciones nacionales y locales;

i) no dejar información critica o sensible en las instalaciones de impresión, como impresoras, copiadoras y faxes, ya que estas pueden ser acezadas por personal no autorizado;

j) los controles y restricciones asociados con el reenvío de las instalaciones de comunicación como por ejemplo el reenvío automático de correos electrónicos a una dirección de correo externa;

k) recordar al personal que deben de tomar precauciones como por ejemplo no revelar información sensible con el fin de evitar ser escuchado o interceptado cuando hagan una llamada telefónica mediante:

1) personas vecinas particularmente cuando se utiliza teléfonos móviles;

2) interceptación de teléfonos y otras formas de oír comunicaciones a través de acceso físico al equipo o a la línea telefónica, o utilizando equipos de recepción de escaneo;

3) personas al final del receptor;

l) no dejar mensajes conteniendo información sensible en las maquinas contestadoras ya que estas pueden ser reproducidas por personas no autorizadas, guardadas en sistemas comunales o grabadas incorrectamente como resultado de un mal discado;

m) recordar al personal sobre los problemas de usar las maquinas de fax, nombrando:

1) el acceso no autorizado para crear almacenes de mensajes con el fin de recuperarlos;

2) la programación deliberada o accidentada de las maquinas para enviar mensajes a números específicos;

3) envío de documentos y mensajes a un numero equivocado por un mal discado o por el uso de un numero mal grabado;

n) recordar al personal no registrar datos demográficos, como la dirección de correo u otra información personal en cualquier software para evitar su uso no autorizado;

o) recordar al personal que los fax modernos y las fotocopiadoras tienen paginas cache y paginas almacenadas en caso de que el papel se trabe y lo imprimirá una vez que se corrija el error.

En adición, el personal debe recordar que no deben de tener conversaciones confidenciales en lugares públicos o en oficinas abiertas y salas de reunión con paredes que no sean aprueba de sonido.

Los recursos de intercambio de información deben concordar con cualquier requisito legal relevante (véase capitulo 15).

Otra Información

El intercambio de información puede ocurrir a través del uso de un numero diferente de tipos de recursos de comunicación, incluyendo correo electrónico, voz, fax y video.

El intercambio de software puede ocurrir a través de un numero diferente de medios, incluyendo descargas desde el Internet y adquisición por medio de vendedores.

Se deben considerar las implicaciones de negocio, legales y de seguridad, asociados con el intercambio electrónico de datos, comercio electrónico, comunicaciones electrónicas y los requerimientos para los controles.

La información puede ser comprometida debido a la falta de precaución, política o procedimientos en el uso de los recursos de intercambio de información, como ser escuchado en un teléfono móvil en un lugar publico, mala dirección de un correo electrónico, maquinas

contestadoras escuchadas, acceso no autorizado a los sistemas de correo de voz y el envío de faxes al equipo equivocado.

Las operaciones de negocio pueden ser interrumpidas y la información puede ser comprometida si las instalaciones de comunicación fallan, se sobrecargan o se interrumpen (véase 10.3 y el capitulo 14). La información puede ser comprometida si es accesada por usuarios no autorizados (véase el capitulo 11).

10.8.2 Acuerdos de Intercambio

Control

Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros.

Guía de Implementación

Los acuerdos de intercambio deben considerar las siguientes condiciones de seguridad:

a) las responsabilidades de la gerencia para controlar y notificar la transmisión, despacho y recibo;

b) procedimientos para notificar al que envía la transmisión, despacho o recibo;

c) procedimientos para asegurar al trazabilidad y la no reproducción;

d) estándares técnicos mínimos para empacado y transmisión;

e) acuerdos de fideicomiso;

f) estándares de identificación de mensajería;

g) responsabilidades en los eventos de los incidentes de la seguridad de información como la perdida de datos;

h) uso de un sistema acordado de etiquetado para información sensible o critica, asegurando que los significados de las etiquetas sea entendido de inmediato y que la información sea protegida apropiadamente;

i) las propiedades y responsabilidades de la protección de datos, copyright, conformidad de la licencia de software y consideraciones similares (véase 15.1.2 y 15.1.4);

j) estándares técnicos para grabar y leer información y software;

k) cualquier control especial que pueda ser requerido para proteger ítems sensibles como las llaves criptográficas (véase el inciso 12.3).

Las políticas, procedimientos y estándares deben ser establecidos y mantenidos para proteger información y medios físicos en transito (véase el inciso 10.8.3) y deben ser referenciados en los acuerdos de intercambio.

La contenido de seguridad de cualquier acuerdo debe reflejar la sensibilidad de la información de negocios envuelta.

Otra Información

Los acuerdos pueden ser electrónicos o manuales y pueden tomar la forma de contratos formales o condiciones de empleo. Para la información sensible, los mecanismos específicos usados para el intercambio de dicha información deben ser consistentes para todas las organizaciones y tipos de acuerdo.

10.8.3 Medios físicos en tránsito

Control

Los medios conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.

Guía de Implementación

Las siguientes pautas deben ser considerada para proteger medios de información transportados entre lugares:

La información puede ser vulnerable a accesos no autorizados, a mal uso o a corrupción durante su transporte físico. Se deberían aplicar los siguientes controles y medidas para salvaguardar los medios informáticos transportados entre sedes:

a) deberían usarse transportes o mensajeros fiables;

b) debería convenirse entre las gerencias una lista de mensajeros autorizados.;

c) se debería realizar un procedimiento para comprobar la identificación de los mensajeros utilizados;

d) el envase debería ser suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito, de acuerdo con las especificaciones de los fabricantes, por ejemplo protegiéndonos contra cualquier factor ambiental que pueda reducir la efectividad de la restauración del medio como una exposición al calor, humedad o a campos electromagnéticos;

e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas, por ejemplo:

1) uso de contenedores cerrados;

2) entrega en mano;

3) envase con detección de apertura (que revela cualquier intento de acceso);

4) en casos excepcionales, fraccionamiento del envío en varías entregas que se envían por rutas diferentes;

Otra Información

La información puede ser vulnerable a los accesos no autorizados, al mal uso o corrupción durante el transporte físico, para instancias en donde se envíe medios vía servicio postal o vía mensajería.

10.8.4 Seguridad en la mensajería electrónica

Control

La información implicado con la mensajería electrónica debe ser protegida apropiadamente.

Guía de Implementación

Las consideraciones de seguridad para la mensajería electrónica deberían incluir lo siguiente:

a) protección de mensajes de accesos no autorizados, modificaciones o negación del servicio;

b) asegurar una dirección y un transporte correcto del mensaje;

c) confiabilidad y disponibilidad general del servicio;

d) consideraciones legales, por ejemplo los requisitos para firmas electrónicas;

e) obtención de aprobación antes de utilizar servicios externos públicos como mensajería instantánea o archivos compartidos;

f) niveles mas fuertes de autentificación del acceso de control de redes publicas accesibles.

Otra Información

La mensajería electrónica como los correos, el intercambio electrónico de datos y la mensajería instantánea, juegan un papel importante en las comunicaciones de negocios. La mensajería electrónica tiene diferentes riesgos que las comunicaciones en papel.

10.8.5 Sistemas de Información de Negocios

Control

Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios.

Guía de Implementación

Las consideraciones dadas a la seguridad e implicaciones de seguridad de interconectar dichas instalaciones, deben incluir:

a) vulnerabilidades conocidas en los sistemas de administración y contabilidad donde la información es compartida por diferentes partes de la organización;

b) vulnerabilidades de información en sistemas de comunicación de negocios, como el grabado de llamadas telefónicas o de conferencia, las llamadas confidenciales, el almacenamiento de faxes, el correo abierto, la distribución de correo;

c) políticas y controles apropiados para manejar información compartida;

d) excluir categorías de información de negocios sensible y clasificar documentos si los sistemas no proveen un nivel apropiado de protección (véase el inciso 7.2);

e) acceso restringido a la información diaria relacionado con individuos selectos, como el personal que trabaja en proyectos sensibles;

f) categorías de personal, contratistas o socios de negocios a los que se les permite el uso del sistema y de las locaciones desde donde puede ser accesado (véase 6.2 y 6.3);

g) instalaciones restringidas seleccionadas para categorías de usuario especificas;

h) identificación del estado de usuarios, como los empleados de la organización o contratistas en los directorios para beneficio de otros usuarios;

i) retención y soporte de la información colgada en el sistema (véase el inciso 10.5.1);

j) requisitos en el retraso y en los arreglos (véase capitulo 14).

Otra Información

Los sistemas de información de oficinas son oportunidades para una rápida diseminación y el compartir información de negocio usando una combinación de: documentos, computadores, computadores móviles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios/instalaciones postales y maquinas de fax.

10.9 Servicios de correo electrónico

OBJETIVO: Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

Las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea y los requisitos para los controles. La integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad deben ser también consideradas.

10.9.1 Comercio Electrónico

Control

La información envuelta en el comercio electrónico pasando a través de redes publicas, deben ser protegidas de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada.

Guía de Implementación

Las consideraciones de seguridad para el comercio electrónico debe incluir lo siguiente:

a) el nivel de confidencia que cada parte requiere en la identidad demanda;

b) los procesos de autorización asociados con el que puede designar los precios, ediciones o firmas en los documentos de negocio;

c) asegurar que los socios de negocio se encuentran totalmente informados de sus autorizaciones;

d) determinar los requerimientos de confidencialidad, integridad, prueba de despacho y recepción de los documentos clave y la no negación de contratos, como por ejemplo los que están asociados con los procesos de ofrecimiento y contrato;

e) el nivel de confianza requerido en la integridad de las listas de precio anunciadas;

f) la confidencialidad de cualquier dato o información sensible,

g) la confidencialidad e integridad de cualquier orden de transacción, información de pago, detalles de direcciones de entrega y confirmaciones de recibos.

h) el grado de verificación apropiado para verificar la información de pago suministrada por un cliente;

i) selección de la forma de establecimiento de pago más apropiada con el fin de evitar fraudes;

j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de orden;

k) evitar la pérdida o duplicidad de la información de transacciones;

l) confiabilidad asociada con cualquier transacción fraudulenta;

m) requisitos de seguro.

Muchas de las consideraciones mencionadas anteriormente pueden ser anexadas por la aplicación de controles criptográficos (véase el inciso 12.3), tomando en cuenta la conformidad con los requisitos legales (véase el inciso 15.1, especialmente 15.1.6 para la legislación criptográfica).

Los arreglos de comercio electrónico entre los socios del negocio deben ser apoyados por un acuerdo documentado que comprometa ambas partes a aceptar los términos de intercambio, incluyendo los detalles de autorización (véase b) arriba). Se pueden necesitar otros acuerdos con servicio de información y valor agregado a las redes de los proveedores.

El sistema público de intercambio debe publicar sus términos de negocio a los clientes.

Se debe dar consideración para la resistencia al ataque de host(s) utilizado para el comercio electrónico y las implicancias de seguridad de cualquier red de interconexión requerida para la implementación de servicios de comercio electrónico (véase el inciso 11.4.6).

Otra Información

El comercio electrónico es vulnerable a un número de amenazas de red que pueden resultar en actividad fraudulenta, disputas de contrato y acceso o modificación de la información.

El comercio electrónico puede hacer uso de métodos seguros de autentificación, como el uso de firmas digitales (véase el inciso 12.3) para reducir riesgos. Igualmente, se puede utilizar personal externo confiable donde sus servicios sean requeridos.

10.9.2 Transacciones en línea

Control

La información implicada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, ruta equivocada, alteración no autorizada de mensajes, acceso no autorizado, duplicado no autorizado del mensaje o reproducción.

Guía de Implementación

Las consideraciones de seguridad para las transacciones en línea deben incluir lo siguiente:

a) el uso de firmas electrónicas por cada una de las partes envueltas en la transacción;

b) todos los aspectos de la transacción, asegurando que:

1) las credenciales de usuario de todas las partes son validas y verificadas;
2) la transacción quede confidencial;
3) la privacidad asociada con todas las partes es retenida

c) los medios de comunicación entre todas las partes implicadas deben ser cifrados;

d) los protocolos utilizadas para comunicarse entre todas las partes debe ser seguro;

e) asegurar que el almacenamiento de los detalles de la transacción estén localizados fuera de cualquier ambiente publico, como en un plataforma de almacenamiento existente en el Intranet de la organización, y que no sea retenida ni expuesta en un medio de almacenamiento al que se puede acceder por Internet;

f) cuando una autoridad confiable sea usada (para propósitos de publicar o mantener firmas digitales y/o certificados digitales) la seguridad es integrada a través de todo proceso de gestión del certificado/firma.

Otra Información

El grado de los controles adoptados necesitará ser conmensurado con el nivel de riesgo asociado con cada forma de la transacción en línea.

Las transacciones pueden necesitar que sean conformes con las leyes, reglas y regulaciones en la jurisdicción en donde la transacción sea generada.

Existen muchas formas de transacciones como las contractuales o financieras, que pueden ser realizadas en línea.

10.9.3 Información publica disponible

Control

La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas.

Guía de Implementación

Software, datos y otra información que requiera un alto nivel de integridad y que se encuentre disponible en un sistema publico, debe ser protegido mediante un mecanismo apropiado como firmas digitales (véase 12.3). El sistema de publicación accesible debe ser probado contra debilidades y fallas antes de que la información se encuentre disponible.

Debe existir un proceso formal aprobado antes de que la información este públicamente disponible. En adición, todos los ingresos provistos desde el exterior al sistema deben ser verificados y aprobados.

Los sistemas de publicación electrónicos deben ser controlados cuidadosamente, especialmente los que permiten retroalimentación e ingreso directo de la información, con el fin de que:

a) la información obtenida concuerde con cualquier legislación de protección de datos (véase el inciso 15.1.4);

b) el ingreso y procesamiento de información en el sistema será procesado completamente y actualizado a tiempo;

c) la información sensible será protegida durante la recolección, procesamiento y almacenamiento;

d) el acceso al sistema público no permite el ingreso involuntario a redes a las que el sistema se encuentre conectado.

Otra Información

La información en un sistema publico disponible, como por ejemplo la información en servidor Web accesible vía Internet, puede necesitar que sea conforme con las reglas, leyes y regulaciones de la jurisdicción en donde dicho sistema se encuentra localizado, donde el intercambio se esta llevando a cabo o donde el propietario resida. Las modificaciones no autorizadas de la información publicada pueden dañar la reputación de la organización publicadora.

10.10 Monitoreo

OBJETIVO: Detectar las actividades de procesamiento de información no autorizadas.

Los sistemas deben ser monitoreados y los eventos de la seguridad de información deben ser grabadas. El registro de los operadores y el registro de averías debe ser usado para asegurar que los problemas del sistema de información sean identificados.

Una organización debe cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.

El monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política.

10.10.1 Registro de la auditoria

Control

Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.

Guía de Implementación

Los registros de auditoria deben incluir, cuando sea relevante:

a) identificaciones de usuarios;

b) fecha y hora de conexión y desconexión;

c) identidad del terminal o locación si es posible;

d) registros de éxito y fracaso de los intentos de acceso al sistema;

e) registros de éxito o fracaso de datos y de otros intentos de acceso a recursos;

f) cambios en la configuración del sistema;

g) uso de privilegios;

h) uso de las instalaciones y aplicaciones del sistema;

i) archivos accesados y el tipo de acceso;

j) direcciones de red y protocolos;

k) las alarmas realizadas por el sistema de control de accesos;

l) activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos.

Otra Información

Los registros de auditoria deben contener datos personales confidenciales. Se deben tomar en cuenta medidas apropiadas para la protección de la privacidad (véase el inciso 15.1.4). Donde sea posible, los administradores del sistema no deben de tener permiso para borrar o desactivar los registros de sus propias actividades (véase el inciso 10.1.3).

10.10.2 Monitoreando el uso del sistema

Control

Los procedimientos para el uso del monitoreo de las instalación de procesamiento de información deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente.

Guía de Implementación

El nivel de monitoreo requerido para las instalaciones individuales debe ser determinado por una evaluación de riesgos. Una organización debe cumplir con todos los requerimientos legales aplicables a sus actividades de monitoreo. Las áreas que deben ser consideradas incluyen:

a) acceso autorizado, incluyendo detalles como:

1) la identificación del usuario;

2) la fecha y hora de los eventos clave;

3) el tipo de evento;

4) los archivos ingresados;

5) el programa e recurso utilizados;

b) todas las operaciones privilegiadas, como:

1) uso de cuentas privilegiadas, como supervisores, administradores;

2) puesta en marcha y parada del sistema;

3) conexión o desconexión de un recurso de entrada o salida;

c) intentos de acceso no autorizado, como:

1) intentos fallidos;
2) acciones con fallas o rechazadas que involucran datos y otros recursos;

3) violaciones a la política de acceso y las notificaciones de los firewalls y entradas de red;

4) las alertas de los sistemas de detección de intrusos del propietario;

d) alertas o fallas del sistema como:

1) alertas o mensajes de consola;

2) excepciones de registro en el sistema;

3) alarmas de la gerencia de red;

4) alarmas levantadas por los sistemas de control de accesos;

e) cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad.

El numero de veces que deberán ser revisados las actividades de monitoreo debe depender de los riesgos implicados. Los factores de riesgo que deben ser considerados incluyen:

a) criticidad de los procesos de aplicación;

b) valor, sensibilidad y criticidad de la información implicada;

c) experiencias pasadas de infiltraciones del sistema y mal uso y la frecuencia de la vulnerabilidades explotadas;

d) extensión de la interconexión del sistema (particularmente redes publicas);

e) registro de la instalación que esta siendo desactivada.

Otra Información

El uso de procedimientos de monitoreo son necesarios para asegurar que los usuarios solo realicen actividades que han sido explícitamente autorizadas.

Una revisión del registro implica un entendimiento de las amenazas enfrentadas por el sistema y la manera en que estas se presentan. Ejemplos de eventos que puedan requerir investigación futura en caso de incidentes en la seguridad de información están dados en 13.1.1.

10.10.3 Protección de la información de registro

Control

Las instalaciones de información de registro deben ser protegidas contra acciones forzosas u acceso no autorizado.

Guía de Implementación

Los controles deben proteger contra cambios no autorizados y problemas operacionales con la instalación de registro incluyendo:

a) alteraciones a los tipos de mensaje que son grabados;

b) archivos de registro editados o eliminados;

c) la capacidad de almacenamiento del medio del archivo de registro que ha sido excedido, resultando en la falla de los eventos almacenados o la sobre escritura de eventos pasados.

Algunos registros de auditoria pueden requerir ser archivados como parte de la política de retención de registros o debido a los requerimientos para recolectar y mantener evidencia (véase el inciso 13.2.3).

Otra Información

Los registros del sistema contienen un volumen largo de información, mucho del cual es extraño para el monitoreo de seguridad. Para ayudar a identificar eventos significativos para propósitos del monitoreo de seguridad, se deben considerar el copiado de tipos de mensajes

apropiados automáticamente a un segundo registro y/o el uso de utilidades adecuadas del sistema o las herramientas de auditoria para realizar la interrogación del archivo y la nacionalización.

Los registros del sistema necesitan ser protegidos debido a que si los datos pueden ser modificados o eliminados, su existencia puede crear una falsa sensación de seguridad.

10.10.4 Registro de administradores y operadores

Control

Las actividades del administrador y de los operadores del sistema deben ser registradas.

Guía de Implementación

Los registros deben incluir:

a) el tiempo en el que ocurrió el evento (éxito o fracaso);

b) información acerca del evento o fallas;

c) que cuenta y que administrador u operador fue implicado;

d) que procesos fueron implicados;

Los registros de los administradores y usuarios del sistema deben ser revisados en una base regular.

Otra Información

Un sistema de detección de intrusos manejado fuera del control del sistema y de las redes de administradores puede ser utilizado para monitorear y dar conformidad a las actividades.

10.10.5 Registro de la avería

Control

Las averías deben ser registradas, analizadas y se debe tomar acciones apropiadas.

Guía de Implementación

Las averías reportadas por usuarios o por programas del sistema relacionados con problemas en el procesamiento o comunicación de la información, deben ser registradas. Deben existir reglas claras para maniobrar las averías reportadas incluyendo:

a) revisión de los registros de averías para asegurar que las fallas han sido resueltas satisfactoriamente;

b) revisión de las medidas correctivas para asegurar que los controles no han sido comprometidos y que la acción realizada es totalmente autorizada.

Se debe asegurar que el registro de error este activado, si es que se encuentra disponible en el sistema.

Otra Información

Los registros de errores y averías pueden impactar en el desarrollo del sistema. Este registro debe ser habilitado por personal competente y el nivel de registro requerido para sistemas individuales debe ser determinado por una evaluación de riesgos, tomando en cuenta la degradación del funcionamiento.

10.10.6 Sincronización del reloj

Control

Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo.

Guía de Implementación

Donde una computadora o un dispositivo de comunicación tenga la capacidad de operar con un reloj en tiempo real, este reloj debe ser instalado con un estándar acordado, como el Tiempo Coordinado Universal o un estándar local de tiempo. Debido a que muchos relojes son conocidos por variar en el tiempo, debe existir un procedimiento que verifique y corrija cualquier variación significativa.

La interpretación correcta del formato tiempo/fecha es importante para asegurar que se refleje el tiempo/fecha correcto. Las especificaciones locales deben ser tomadas en cuenta.

Otra Información

Los ajustes correctos en los relojes de las computadoras son importantes debido a que aseguran la exactitud de los registros de auditoria, que pueden ser requeridos para investigaciones o como evidencia en casos legales o disciplinarios. Los registros de auditoria inexactos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dicha evidencia. Un reloj vinculado a un broadcast de radio de tiempo desde un reloj atómico nacional puede ser utilizado como el reloj maestro para los sistemas de registro. Un protocolo de tiempo de red puede ser usado para mantener todos los servidores en sincronización con el reloj maestro.

11. CONTROL DE ACCESOS

11.1 Requisitos de negocio para el control de accesos

OBJETIVO: Controlar los accesos a la información.

Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio.

Se deberían tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

11.1.1 Política de control de accesos

Control

Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.

Guía de implementación

Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. Los controles de acceso son lógicos y físicos (véase el capitulo 9) y estos deben ser considerados juntos. Se debería dar a los usuarios y proveedores de

servicios una especificación clara de los requisitos de negocio cubiertos por los controles de accesos.

Esta política debería contemplar lo siguiente:

a) requisitos de seguridad de cada aplicación de negocio individualmente;

b) identificación de toda la información relativa a las aplicaciones y los riesgos que la información esta enfrentando;

c) políticas para la distribución de la información y las autorizaciones (por ejemplo, el principio de suministro sólo de la información que se necesita conocer y los niveles de seguridad para la clasificación de dicha información) (véase el inciso 7.2);

d) coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes;

e) legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios (véase el inciso 15.1);

f) perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos;

g) administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión;

h) segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos;

i) requerimientos para la autorización formal de los pedidos de acceso (véase el inciso 11.2.1);

j) requerimientos para la revisión periódica de los controles de acceso (véase el inciso 11.2.4);

k) retiro de los derechos de acceso (véase el inciso 8.3.3).

Otra Información

Al especificar las reglas de los controles de accesos se tendrá la precaución de considerar:

a) la distinción entre reglas a cumplir siempre y reglas opcionales o condicionales;

b) el establecimiento de las reglas basándose en la premisa "está prohibido todo lo que no esté permitido explícitamente", premisa que es contraria a la regla "está permitido todo lo que no esté prohibido explícitamente", considerada más débil o más permisiva.

c) los cambios en las etiquetas de información (véase el inciso 7.2) iniciadas automáticamente por los recursos del tratamiento de la información y las que inicia el usuario manualmente;

d) los cambios en las autorizaciones al usuario realizados automáticamente por el sistema de información y los que realiza un administrador;

e) la distinción entre reglas que requieren o no la aprobación del administrador o de otra autoridad antes de su promulgación.

Las reglas de control de acceso deben ser apoyadas por procedimientos formales y por responsabilidades claramente definidos (véase, por ejemplo, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Gestión de acceso de usuarios

OBJETIVO: Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

Se debería establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debería prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

11.2.1 Registro de usuarios

Control

Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

Guía de Implementación

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro que debería incluir:

a) la utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debería permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados;

b) la comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información. También puede ser conveniente que la gerencia apruebe por separado los derechos de acceso;

c) verificación de la adecuación del nivel de acceso asignado al propósito del negocio (véase el inciso 11.1) y su consistencia con la política de seguridad de la organización (por ejemplo, su no contradicción con el principio de segregación de tareas (véase el inciso10.1.3);

d) la entrega a los usuarios de una relación escrita de sus derechos de acceso;

e) la petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso;

f) la garantía de que no se provea acceso al servicio hasta que se hayan completado los procedimientos de autorización;

g) el mantenimiento de un registro formalizado de todos los autorizados para usar el servicio;

h) la eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella;

i) la revisión periódica y eliminación de identificadores y cuentas de usuario redundantes (véase el inciso 11.2.4);

j) la garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

Otra Información

Se debería considerar el establecimiento de roles de acceso a usuario basado en requisitos de negocio que resuman un numero de derechos de acceso en un expediente típico de acceso de

usuario. Los pedidos y revisiones de acceso (véase el inciso 11.2.4) son manejadas mas fácilmente al nivel de dichos roles que los niveles de derechos particulares.

Se debería considerar la inclusión de cláusulas en los contratos laborales y de servicio que especifiquen sanciones si sus signatarios realizan accesos no autorizados (véase el inciso 6.1.4 y 6.1.5).

11.2.2 Gestión de privilegios

Control

Debería restringirse y controlarse el uso y asignación de privilegios.

Guía de Implementación

Se debería controlar la asignación de privilegios por un proceso formal de autorización en los sistemas multiusuario. Se deberían considerar los pasos siguientes:

a) identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación; así como las categorías de empleados que necesitan de ellos;

b) asignar privilegios a los individuos según los principios de “necesidad de su uso” y “caso por caso” y en línea con la política de control de acceso (véase el inciso 11.1.1), por ejemplo, el requisito mínimo para cumplir su función sólo cuando se necesite;

c) mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido;

d) promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios;

e) promover el desarrollo y uso de programas que evitan la necesidad de correr con privilegios;

f) asignar los privilegios a un identificador de usuario distinto al asignado para un uso normal.

Otra información

Un uso inapropiado de los privilegios de la administración del sistema (cualquier característica o facilidad de un sistema de información que habilite al usuario sobrescribir los controles del sistema o de la aplicación) pueden ser un gran factor contribuidor de fallas o aberturas en los sistemas.

11.2.3 Gestión de contraseñas de usuario

Control

Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal.

Guía de Implementación

El proceso debe incluir los siguientes requisitos:

a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo (compromiso que podría incluirse en los términos y condiciones del contrato de empleo, véase el inciso 8.1.3);

b) proporcionar inicialmente una contraseña temporal segura (véase el inciso 11.3.1) que forzosamente deben cambiar inmediatamente después;

c) establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de reemplazo o temporal;

d) establecer un conducto seguro para hacer llegar las contraseñas temporales a los usuarios. Se debería evitar su envío por terceros o por mensajes no cifrados de correo electrónico;

e) las contraseñas temporales deben ser únicas para cada individuo y no deben ser obvias;

f) los usuarios deberían remitir acuse de recibo de sus contraseñas;

g) las contraseñas nunca deben ser almacenadas en sistemas de cómputo sin ser protegidos;

h) las contraseñas por defecto de los vendedores deben ser alteradas después de la instalación de los sistemas o software.

Otra Información

Las contraseñas son un medio común de verificar la identidad del usuario antes de que el acceso a un sistema de información o servicio sea dado de acuerdo a la autorización del usuario. Se deben considerar, si son apropiadas, otras tecnologías para identificación y autentificación de usuario como las biométricas (como la verificación de huellas, la verificación de la firma) o el uso de dispositivos hardware (como las tarjetas inteligentes).

11.2.4 Revisión de los derechos de acceso de los usuarios

Control

La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios.

Guía de Implementación

La revisión de los derechos de acceso de usuario debería considerar las siguientes pautas:

a) revisar los derechos de acceso de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses) y después de cualquier cambio como promoción, degradación o termino del empleo (véase el inciso 11.2.1);

b) los derechos de acceso de los usuarios deben ser revisados y reasignados cuando se traslade desde un empleo a otro dentro de la misma organización;

c) revisar más frecuentemente (se recomienda cada tres meses) las autorizaciones de derechos de acceso con privilegios especiales (véase el inciso 11.2.2);

d) comprobar las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados;

e) los cambios en las cuentas privilegiadas deben ser registradas para una revisión periódica.

Otra Información

Es necesario revisar regularmente los derechos de los accesos de los usuarios para mantener un control efectivo del acceso a los datos y los sistemas de información.

11.3 Responsabilidades de los usuarios

OBJETIVO: Evitar el acceso de usuarios no autorizados y el compromiso o hurto de la información y de las instalaciones del procesamiento de información.

Una protección eficaz necesita la cooperación de los usuarios autorizados.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Un escritorio limpio, así como una política de pantalla clara debe ser implementado con el fin de reducir el riesgo de acceso no autorizado o de daño a los papeles, medios e instalaciones del procesamiento de información.

11.3.1 Uso de contraseñas

Control

Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

Guía de Implementación

Todos los usuarios deberían ser informados acerca de:

a) mantener la confidencialidad de las contraseñas;

b) evitar guardar registros (papel, archivos de software o dispositivos) de las contraseñas, salvo si existe una forma segura de hacerlo y el método de almacenamiento ha sido aprobado;

c) cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema;

d) seleccionar contraseñas de buena calidad, con una longitud mínima caracteres, que sean:

1) fáciles de recordar;

2) no estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario, por ejemplo, nombres, fechas de nacimiento, números de teléfono, etc.;

3) no sean vulnerables a ataques de diccionario (no consisten en palabras incluidas en diccionarios);

4) estén carentes de caracteres consecutivos repetidos o que sean todos números o todas letras;

e) cambiar las contraseñas a intervalos de tiempo regulares o en proporción al número de accesos (las contraseñas de las cuentas con privilegios especiales deberían cambiarse con más frecuencia que las normales), evitando utilizar contraseñas antiguas o cíclicas;

f) cambiar las contraseñas temporales asignadas para inicio, la primera vez que se ingrese al sistema;

g) no incluir contraseñas en ningún procedimiento automático de conexión, que, las deje almacenadas permanentemente;

h) no compartir contraseñas de usuario individuales.

i) no utilizar la misma contraseña para propósitos personales o de negocio.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se les pide que mantengan contraseñas múltiples, deberían ser aconsejados sobre la posibilidad de usar una sola contraseña de calidad (véase el punto anterior d) para todos los servicios, que brinde un nivel razonable de protección para la contraseña almacenada.

Otra Información

La gestión de los sistemas de ayuda que tratan con problemas de perdida u olvido de contraseña necesitan un cuidado especial ya que esto también significa medios de ataque al sistema de contraseñas.

11.3.2 Equipo informático de usuario desatendido

Control

Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos.

Guía de Implementación

Todos los usuarios y proveedores de servicios deberían conocer los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos, así como sus responsabilidades para implantar dicha protección. Se les debería recomendar:

a) cancelar todas las sesiones activas antes de marcharse, salvo si se dispone de una herramienta de bloqueo general, por ejemplo, una contraseña para protector de pantalla;

b) desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión (y no sólo apagar el terminal o el computador personal);

c) proteger el terminal o el puesto de trabajo cuando no estén en uso con un bloqueador de teclado o una medida similar, por ejemplo, una contraseña de acceso (véase el inciso 11.3.3).

Otra Información

El equipo instalado en áreas de usuarios, como las estaciones de trabajo o los servidores de archivo, pueden requerir protección especifica para un acceso no autorizado cuando se desatienda por un periodo extenso.

11.3.3 Política de pantalla y escritorio limpio

Control

Se debería adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento así como una política de pantalla limpia para instalaciones de procesamiento de información.

Guía de Implementación

La política de pantalla y escritorio limpio debe tomar en cuenta la clasificación de la información (véase el inciso 7.2), los requerimientos legales y contractuales (véase el inciso

15.1), los riesgos correspondientes y los aspectos culturales de la organización. Las siguientes pautas deben ser consideradas:

a) la información critica o sensible del negocio (papel o medios electrónicos de almacenamiento) debe ser asegurada (seria ideal un caja fuerte, gavetas u otras formas de muebles de seguridad) cuando no sea requerido, especialmente cuando la oficina este vacía;

b) los computadores y terminales deben ser apagados o protegidos con un mecanismo de protección de pantalla o de teclado controlado por contraseña u otro mecanismo de autentificación, cuando estas se encuentren desatendidos y deben ser protegidas por cerraduras clave, contraseñas u otro tipo de control cuando no sean utilizados;

c) los puntos salientes o entrantes de correo y los faxes desatendidos deben ser protegidos;

d) debe ser prevenido el uso no autorizado de fotocopiadoras y otras tecnologías de reproducción como scanner o cámaras digitales;

e) los documentos que contienen información sensible y clasificada deben ser removidos de las impresoras de inmediato.

Otra Información

Una política de pantalla y escritorio limpio reduce los riegos de un acceso no autorizado y de la perdida o daño de la información durante horas de trabajo no establecidas. Las cajas fuertes u otras formas de instalaciones de almacenamiento pueden también proteger información almacenada contra desastres como incendio, terremotos, inundación u explosión.

Considere el uso de impresoras con código pin de modo tal que los creadores sean los únicos que puedan sacar sus impresiones y solo cuando se encuentren al costado de la impresora.

11.4 Control de acceso a la red

OBJETIVO: Prevenir el acceso no autorizado de los servicios de la red.

Debería controlarse el acceso a los servicios a las redes internas y externas.

Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

a) interfaces adecuadas entre la red de la organización y las redes públicas o las privadas de otras organizaciones;

b) mecanismos adecuados de autenticación para los usuarios y los equipos;

c) control de los accesos de los usuarios a los servicios de información

11.4.1 Política de uso de los servicios de la red

Control

Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica.

Guía de Implementación

Se debería formular la política de uso de las redes y los servicios de la red, que es conveniente que cubra:

a) las redes y los servicios de la red a los que se puede acceder;

b) los procedimientos de autorización para determinar quién puede acceder a qué redes y a qué servicios de la red;

c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de las redes y a los servicios de la red;

d) los medios usados para el acceso y los servicios de red (las condiciones para permitir el acceso por discado al proveedor de servicio de Internet o a un sistema remoto).

La política debería ser coherente con la política de control de accesos de la organización (véase el inciso 11.1).

11.4.2 Autentificación de usuario para conexiones externas

Control

Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos.

Guía de Implementación

La autentificación de usuarios remoto puede realizarse utilizando, por ejemplo, una técnica basada en criptografía, símbolos de hardware o un protocolo de desafío/respuesta. Se pueden encontrar posibles implementaciones de dichas técnicas en varias soluciones de redes privadas virtuales. También se pueden utilizar líneas privadas dedicadas, con el fin de proveer aseguramiento en la fuente de conexiones.

Los procedimientos y controles de dial-back por ejemplo, usando módems de dial-back, pueden ofrecer protección contra conexiones no autorizadas ni deseadas a los recursos de tratamiento de información de una organización. Este tipo de control autentica a los usuarios que tratan de establecer conexión a la red de la organización desde lugares remotos. Cuando se usa este control, la organización no debería usar servicios de red que incluyan reexpedición de llamadas y si la tienen, deberían desconectarla para evitar la debilidad consecuente. También es importante que el proceso de dial-back asegure la desconexión del lado de la organización. Si no, el usuario remoto podría mantener la línea abierta pretendiendo que se ha verificado el dial-back. Los procedimientos y controles de dial-back deberían pasar pruebas para evitar esta posibilidad.

Un nodo de autentificación puede servir como un medio alternativo para autentificar grupos de usuarios remotos donde estén conectados a un computador seguro. Las técnicas criptográficas, basados en certificados de maquinas, pueden ser utilizados para autentificar nodos.

Controles adicionales de autentificación deben ser implementados para el control de acceso de redes inalámbricas. En particular, se requiere especial cuidado en la selección de controles para redes inalámbricas debido a las grandes oportunidades de intercepciones no detectadas e inserciones de tráfico en la red.

Otra información

Las conexiones externas proveen un potencial acceso no autorizado a la informacion del negocio, como los accesos mediante métodos de discado. Existen diferentes tipos de métodos de autentificación y algunos pueden proveer un mayor nivel de protección que otros, como por ejemplo los métodos basados en técnicas criptográficas las cuales pueden proveer una fuerte autentificación. Es importante determinar, desde una evaluación de riesgos, el nivel de protección requerida. Esto es necesario para la apropiada selección de un método de autentificación.

Una instalación para una conexión automática a un computador remoto puede proveer una forma de ganar acceso no autorizado a una aplicación de negocio. Estos es especialmente importante si la conexión usa una red que se encuentra fuera del control de la gestión de seguridad de la organización.

11.4.3 Identificación de equipos en las redes

Control

Las identificaciones automáticas de equipo deben ser consideradas como medios para autentificar conexiones desde locales y equipos específicos.

Guía de Implementación

La identificación de equipos puede ser utilizada si es importante que las comunicaciones puedan ser iniciadas desde un local y equipo especifico. Un identificador dentro o adjunto al equipo puede ser utilizado para indicar si el equipo esta autorizado para conectarse a la red. Estos identificadores deben identificar claramente a que redes se pueden conectar los equipos, si existe más de una red y particularmente si estas redes son de sensibilidad diferida. Puede ser necesario considerar protección física del equipo con el fin de mantener la seguridad de los identificadores del equipo.

Otra Información

Este control puede ser complementado con otras técnicas para autentificar el usuario del equipo (véase 11.4.2). La identificación de los equipos puede ser aplicado adicionalmente a la identificación de usuarios.

11.4.4 Diagnostico remoto y configuración de protección de puertos

Control

Se debería controlar el acceso físico y logístico para diagnosticar y configurar puertos.

Guía de Implementación

Controles potenciales para el acceso de diagnostico y configuración de puertos incluyen el uso de un cierre con llave y de procedimientos de apoyo para controlar el acceso físico al puerto.

Un ejemplo para dicho procedimientos de apoyo es asegurar que el diagnostico y configuración de puertos sean solo accesibles por arreglo entre el director del servicio de computo y el personal de mantenimiento de hardware/software que requiere acceso.

Los puertos, servicios e instalaciones similares instaladas en una computadora o instalación de computo que no son requeridas específicamente para la funcionalidad del negocio, debe ser inhabilitado o removido.

Otra Información

Muchos sistemas de computo, sistemas de red y de comunicación son instaladas con un diagnostico remoto o instalación de configuración para uso de ingenieros de mantenimiento. Si se encuentra desprotegida, el diagnostico de puertos provee medios de acceso no autorizado.

11.4.5 Segregación en las redes

Control

Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes.

Guía de Implementación

Un método para controlar la seguridad de grandes redes es dividirlas en dominios lógicos separados (por ejemplo dominios de redes internas a la organización o de redes externas), cada uno protegido por un perímetro definido de seguridad. Se puede aplicar un conjunto graduado de controles en diferentes dominios de redes lógicas para segregar a futuro los ambientes de seguridad de red, como por ejemplo sistemas públicos accesibles, redes internas y activos críticos. Los dominios deben ser definidos basados en una evaluación de riesgos y los diferentes requisitos de seguridad entre cada uno de los dominios.

Entre las dos redes a interconectar puede implantarse como perímetro un gateway seguro que controle los accesos y los flujos de información entre los dominios. Se debería configurar este gateway para que filtre el tráfico entre ellos (véanse los incisos 11.4.6 y 11.4.7) y bloquee los accesos no autorizados de acuerdo con la política de control de accesos de la organización (véase el inciso 11.1). Un ejemplo de este tipo de gateway es lo que comúnmente se conoce como firewall. Otro método de segregar dominios lógicos es restringir el acceso a red utilizando redes virtuales privadas para usuarios de grupos entre las organizaciones.

Las redes pueden ser segregadas también utilizando la funcionalidad de los dispositivos de red como el cambio de IP. Los dominios separados pueden ser implementados después controlando los flujos de datos utilizando capacidades de enrutamiento como las listas de control de acceso.

Los criterios para segregar las redes en dominios se deberían basar en la política de control de accesos y en los requisitos de acceso (véase el inciso 10.1) teniendo también en cuenta el costo relativo y el impacto en el rendimiento por la incorporación de la tecnología adecuada de enrutamiento de gateway en la red (véanse los incisos 11.4.6 y 11.4.7).

En adición, la segregación de redes en dominios debe ser basado en el valor y clasificación de la información almacenada o procesada en la red, niveles de confianza o líneas de negocio con el fin de reducir el impacto total de una interrupción de servicio.

Se debe tomar consideración con las redes inalámbricas desde una red interna hacia una privada. Como los perímetros de las redes inalámbricas no están bien definidos, se debe llevar a acabo una evaluación de riesgos en dichos casos para identificar controles (una fuerte autentificación, métodos criptográficos y frecuencia de selección) para mantener una segregación de red.

Otra Información

Las redes han sido crecientemente extendidas mas allá de las barreras organizacionales tradicionales, como se forman alianzas de negocios que puedan requerir la interconexión o el compartir las instalaciones de red y de procesamiento de información. Estas extensiones pueden incrementar el riesgo de un acceso no autorizado a los sistemas de información existentes que utilizan la red, algunos de los cuales pueden requerir protección de otros usuarios de redes debido a su sensibilidad o criticidad.

11.4.6 Control de conexión a las redes

Control

Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones del negocio (véase el inciso 11.1).

Guía de Implementación

Los derechos de acceso de los usuarios deben ser mantenidos y actualizados como requiere la política de control de accesos (véase el inciso 11.1.1).

La capacidad de conexión de los usuarios pueden ser restringido a través de entradas que filtren el trafico por medio de tablas o reglas pre definidas. Algunos ejemplos de aplicaciones a las cuales las que se debe aplicar las restricciones son:

a) correo electrónico;

b) transferencia de archivos;

c) acceso interactivo;

d) acceso a la aplicación.

Se debe considerar vincular los derechos de acceso a red en ciertos periodos del día o en fechas.

Otra Información

Puede ser requerida, por la política de control de acceso para redes compartidas, la incorporación de controles para restringir las capacidades de conexión de los usuarios especialmente a través de las fronteras de la organización.

11.4.7 Control de enrutamiento en la red

Control

Se deberían implementar controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones.

Guía de Implementación

Los controles del enrutamiento podrían basarse en mecanismos positivos de verificación de las direcciones de origen y destino de los mensajes.

Las salidas pueden ser utilizadas para validar la fuente y los destinos de los mensajes en puntos de control de redes internas o externas si se utilizan tecnologías de conversión u oto tipo de herramienta similar. Su implementación debería tener en cuenta la robustez de los propios mecanismos empleados. Los requisitos para el enrutamiento de los controles deben estar basados en la política de control de accesos (véase el inciso 11.1).

Otra Información

Las redes compartidas, especialmente las que se extienden a través de las fronteras de la organización, pueden requerir controles de enrutamiento adicionales. Esto aplica particularmente cuando las redes son compartidas con usuarios externos.

11.5 Control de acceso al sistema operativo

OBJETIVO: Evitar accesos no autorizados a los computadores.

Las prestaciones de seguridad a nivel de sistema operativo se deberían utilizar para restringir el acceso a los recursos del computador. Estos servicios deberían ser capaces de:

a) identificar y verificar la identidad de cada usuario autorizado en concordancia con una política definida de control de acceso;

b) registrar los accesos satisfactorios y fallidos al sistema;

c) registrar el uso de privilegios especiales del sistema;

d) alarmas para cuando la política del sistema de seguridad sea abierta;

e) suministrar mecanismos, adecuados de autenticación;

f) cuando proceda, restringir los tiempos de conexión de usuarios

11.5.1 Procedimientos de conexión de terminales

Control

El acceso a los servicios de información debería estar disponible mediante un proceso de conexión seguro.

Guía de Implementación

Se debería diseñar un procedimiento para conectarse al sistema informático que minimice la posibilidad de accesos no autorizados. Por tanto, el proceso de conexión debería mostrar el mínimo posible de información sobre el sistema para no facilitar ayuda innecesaria a usuarios no autorizados. Un buen procedimiento de conexión debería:

a) no mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión;

b) mostrar un mensaje que advierta la restricción de acceso al sistema sólo a usuarios autorizados;

c) no ofrecer mensajes de ayuda durante el proceso de conexión que puedan guiar a usuarios no autorizados;

d) validar la información de conexión sólo tras rellenar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicar qué parte de esos datos es correcta o no;

e) limitar el número de intentos fallidos de conexión (se recomienda tres) y considerar:

1) el registro de los intentos fallidos de conexión;

2) un tiempo forzoso de espera antes de permitir un nuevo intento de conexión o su rechazo sin una autorización específica;

3) la desconexión de la comunicación de datos;

4) el envío de un mensaje de alerta a la consola del sistema si se alcanza el número máximo de oportunidades de conexión;

5) establecer el número de pruebas de contraseña en conjunción con su largo mínimo y el valor de los sistemas que están siendo protegidos;

f) limitar los tiempos máximo y mínimo permitidos para efectuar el proceso de conexión; y concluir si se exceden;

g) mostrar la siguiente información tras completar una conexión con éxito:

1) fecha y hora de la anterior conexión realizada con éxito;

2) información de los intentos fallidos desde la última conexión realizada con éxito.

h) no mostrar la contraseña que se ingresa o considerar esconderla con caracteres simbólicos;

i) no transmitir contraseñas en texto legible a través de la red;

Otra Información

Si las contraseñas son transmitidas en texto legible durante la sesión de conexión, estas pueden ser capturadas por programas "succionadores" de red.

11.5.2 Identificación y autenticación del usuario

Control

Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos.

Guía de Implementación

Este control debe ser aplicado para todos los tipos de usuario (incluidos los administradores de red y de bases de datos, los programadores de sistemas y el personal técnico de apoyo).

Los ID de los usuarios deben ser utilizados para seguir la pista de las actividades de cada responsable individual. Las actividades regulares del usuario no deben ser realizadas desde cuentas privilegiadas.
En circunstancias excepciona1es que se justifiquen por sus ventajas pueden usarse identificadores de usuario compartidos para un grupo de usuarios o un trabajo específico. En estos casos se debería necesitar la aprobación escrita de la gerencia. Puede necesitarse la implantación de controles adicionales para la responsabilidad.

Los ID´s genéricos utilizados por individuos deben ser solo permitidos donde las funciones o acciones llevadas a cabo no requieren ser trazadas (como la lectura) o cuando existan otros controles establecidos (contraseñas genéricas utilizadas solamente por un grupo de personas a la vez y conectándose en dicho momento).

Donde se requiera una fuerte autentificación e identificación, se pueden utilizar métodos alternativos a las contraseñas como medios criptográficos, tarjetas inteligentes o medios biométricos.

Otra Información

Las contraseñas (véase también el inciso 11.3.1 y 11.5.3) son una forma común de conseguir la identificación y la autenticación (I & A) del usuario, están basadas en un secreto que sólo él conoce. Esto mismo también se puede conseguir por medios criptográficos y protocolos de autenticación. La rigidez de la identificación y autentificación de usuarios debe ser adecuada a la sensibilidad de la información a la que se accede.

También puede conseguirse I & A con objetos como tarjetas inteligentes, minicalculadoras con claves almacenables o bien con tecnologías biométricas que utilizan características o atributos únicos de un individuo. Una combinación de tecnologías y mecanismos, relacionados mediante el establecimiento de un enlace seguro, pueden proporcionar una autenticación reforzada o más robusta.

11.5.3 Sistema de gestión de contraseñas

Control

Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas.

Guía de Implementación

Un buen sistema de gestión de contraseñas debería:

a) imponer el uso de contraseñas individuales con el fin de establecer responsabilidades;

b) permitir que los usuarios escojan sus contraseñas, las cambien e incluyan un procedimiento de confirmación para evitar errores al introducirlas;

c) imponer la selección de contraseñas de calidad (véase el inciso 11.3.1);

d) imponer el cambio de contraseñas (véase el inciso 11.3.1);

e) imponer el cambio de contraseñas iniciales en la primera conexión (véase el inciso 11.2.3);

f) mantener un registro de las anteriores contraseñas utilizadas, por ejemplo, durante el último año, e impedir su reutilización;

g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;

h) almacenar las contraseñas y los datos del sistema de aplicaciones en sitios distintos;

i) almacenar las contraseñas en forma cifrada mediante un algoritmo de cifrado unidireccional;

Otra Información

Las contraseñas son uno de los principales medios para validar la autoridad de los usuarios para acceder al servicio de cómputo.
Algunas aplicaciones requieren de contraseñas de usuario para ser asignadas por una autoridad independiente; en dichos casos, los puntos b), d) y e) anteriores no aplican. En la mayoría de los casos las contraseñas son seleccionadas y mantenidas por los usuarios. Véase el inciso 11.3.1 para pautas en el uso de contraseñas.

11.5.4 Utilización de las facilidades del sistema

Control

La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado.

Guía de Implementación

Las siguientes pautas deberían ser consideradas:

a) usar procedimientos de autenticación, identificación y autorización para las facilidades del sistema;

b) separar las facilidades del sistema de las aplicaciones de software;

c) limitar el uso de las facilidades del sistema al mínimo número de usuarios autorizados y fiables (véase también 11.2.2);

d) autorizar el uso de las facilidades con un propósito concreto (ad hoc);

e) limitar la disponibilidad de las facilidades del sistema, por ejemplo, durante un cambio autorizado;

f) registrar (logging) todo uso de las facilidades del sistema;

g) definir y documentar los niveles de autorización para las facilidades del sistema;

h) desactivar o retirar todas las facilidades basadas en software y el software de sistemas que no sean necesarios.

i) no poner en disponibilidad las facilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas donde la segregación de tareas sea requerida.

Otra Información

La mayoría de las instalaciones de cómputo tienen uno o mas programas de facilidades del sistema que pueden ser capaces de eludir los controles del sistema o de las aplicaciones.

11.5.5 Desconexión automática de sesiones

Control

Las sesiones se deberían desactivar tras un periodo definido de inactividad.

Guía de Implementación

Este dispositivo de desactivación debería borrar la pantalla y cerrar la aplicación y las sesiones de conexión a red tras dicho periodo definido de inactividad. El tiempo de desactivación debería reflejar los riesgos de seguridad del área, la clasificación de la información que se maneja, las aplicaciones que se utilizan y los riesgos relacionados con los usuarios de lo equipos.

Muchos computadores personales suelen tener limitado de alguna forma este dispositivo que borra la pantalla para evitar el acceso no autorizado, pero no cierra la aplicación o las sesiones de conexión a red.

Otra Información

Este control es particularmente importante en locaciones con alto riesgo e incluyen áreas públicas o externas fuera de la gestión de seguridad de la organización. La sesión debe ser desactiva para prevenir el acceso por personas no autorizadas.

11.5.6 Limitación del tiempo de conexión

Control

Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.

Guía de Implementación

Estas medidas de control se deberían emplear para aplicaciones sensibles, en especial para terminales instalados en áreas de alto riesgo, las públicas o no cubiertas por la gestión de seguridad de la organización. Restricciones como por ejemplo:

a) el uso de 'ventanas' de tiempo predeterminadas, por ejemplo para transmisiones de archivos en batch, o para sesiones interactivas regulares de corta duración;

b) la restricción de tiempos de conexión al horario normal de oficina, si no existen requisitos para operar fuera de este horario;

c) considerar la re-autentificación en intervalos medidos.

Otra Información

Limitar el periodo durante el cual las conexiones a los servicios de computo están permitidas, reduce la ventana de oportunidad para un acceso no autorizado. Limitar la duración de las sesiones activas previene a los usuarios de mantener su sesión abierta para prevenir la re-autentificación.

11.6 Control de acceso a las aplicaciones y la información

OBJETIVO: Prevenir el acceso no autorizado a la información contenida en los sistemas.

Se deberían usar las facilidades de seguridad lógica dentro de los sistemas de aplicación para restringir el acceso.

Se deberían restringir el acceso lógico al software y a la información sólo a los usuarios autorizados. Las aplicaciones deberían:

a) controlar el acceso de los usuarios a la información y las funciones del sistema de aplicación, de acuerdo con la política de control de accesos;

b) protegerse de accesos no autorizados desde otras facilidades o software de sistemas operativos que sean capaces de eludir los controles del sistema o de las aplicaciones;

c) no comprometer la seguridad de otros sistemas con los que se compartan recursos de información;

11.6.1 Restricción de acceso a la información

Control

Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.

Guía de Implementación

Las restricciones de acceso deben estar basadas en requisitos específicos de la aplicación y consistente con la política de acceso a la información de la organización (véase el inciso 11.1).
Deberían considerarse las siguientes pautas para dar soporte a los requisitos de restricción de accesos:

a) establecer menús para controlar los accesos a las funciones del sistema de aplicaciones;

b) controlar los derechos de acceso de los usuarios, por ejemplo lectura, escritura, borrado, ejecución;

c) controlar los derechos de acceso de otras aplicaciones;

d) asegurarse que las salidas de los sistemas de aplicación que procesan información sensible, sólo contienen la información correspondiente para el uso de la salida y se envían, únicamente, a los terminales y sitios autorizados, incluyendo la revisión periódica de dichas salidas para garantizar la supresión de información redundante.

11.6.2 Aislamiento de sistemas sensibles

Control

Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados).

Guía de Implementación

Algunos sistemas de aplicaciones son tan sensibles a posibles pérdidas que pueden necesitar un tratamiento especial, que corran en un procesador dedicado, que sólo compartan recursos con otros sistemas de aplicaciones garantizados o que no tengan limitaciones. Las consideraciones siguientes son aplicables para el aislamiento de sistemas sensibles:

a) el propietario de la aplicación debería indicar explícitamente y documentar la 'sensibilidad' de ésta (véase el inciso 7.1.2);

b) cuando una aplicación sensible se ejecute en un entorno compartido, se deberían identificar y acordar con su propietario los sistemas de aplicación con los que compartan recursos.

Otra Información

Algunas aplicaciones de sistemas son lo suficientemente sensibles a perdidas potenciales que requieren un tratamiento especial. La sensibilidad puede indicar que la aplicación:

a) debe correr en una computadora dedicada; o

b) debe compartir recursos solamente con aplicaciones confiables.

El aislamiento puede ser alcanzado usando métodos físicos o lógicos (véase el inciso 11.4.5).

11.7 Informática móvil y teletrabajo

OBJETIVO: Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

La protección requerida debería ser proporcional a los riesgos que causan estas formas específicas de trabajo. Se deberían considerar los riesgos de trabajar en un entorno

desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización debería implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

11.7.1 Informática móvil y comunicaciones

Control

Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática.

Guía de Implementación

Se debería tener un especial cuidado para asegurar que la información de negocio no se comprometa cuando se usan dispositivos de informática móvil como portátiles, agendas, calculadoras y teléfonos móviles. Se debería formalizar una política que tenga en cuenta los riesgos de trabajar con dispositivos de informática móvil, especialmente en entornos desprotegidos.

Dicha política debería incluir los requisitos de protección física, controles de acceso, técnicas criptográficas, respaldos y protección antivirus. Esta política también debería incluir reglas y consejos para conectar los dispositivos de informática móvil a las redes así como una guía para el uso de estos dispositivos en lugares públicos. Se debería tener cuidado cuando se usen dispositivos de informática móvil en lugares públicos, salas de reuniones y otras áreas desprotegidas fuera de locales de la organización. Se debería instalar una protección, por ejemplo, usando técnicas criptográficas (véase el inciso 12.3), para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos.

Cuando estos dispositivos se usen en lugares públicos, es importante tener cuidado para evitar el riesgo de que se enteren personas no autorizadas. Se deberían instalar y mantener al día procedimientos contra el software malicioso (véase el inciso10.4).

Se deben realizar regularmente backups de información crítica de negocio. El equipo debe ser capaz de permitir un rápido y fácil backups de información. Estos backup deben tener una protección adecuada contra hurto o perdida de información.

Se debería proteger debidamente el uso de dispositivos de informática móvil conectados a las redes. Sólo se deberían realizar accesos remotos a la información del negocio usando dispositivos de informática móvil y a través de la red pública pasando por los mecanismos

adecuados de control de accesos (véase el inciso 11.4) y después de conseguir con éxito la propia identificación y autenticación.

También se deberían proteger físicamente los dispositivos de informática móvil contra el robo, sobre todo cuando se dejan, por ejemplo, en coches u otros transportes, en habitaciones de hoteles, en centros de conferencias y en lugares de reunión. Se debería establecer un procedimiento adecuado tomando en cuenta requisitos legales, de seguro y otros requisitos de seguridad para los casos de robo o perdida de las instalaciones móviles. No se debería dejar solo, o sin vigilar, un equipo que contenga información importante, sensible y/o crítica; si es posible se debería guardar bajo llave. Puede encontrarse más información sobre protección física de dispositivos de informática móvil en el inciso 9.2.5.

Se debería concienciar al personal que use dispositivos de informática móvil con objeto de aumentar su percepción de los riesgos adicionales que produce esta forma de trabajo y de las medidas y controles a implantar.

Otra Información

Las conexiones móviles inalámbricas son similares a otros tipos de conexiones de red, pero tienen importantes diferencias que deben ser consideradas cuando se identifican los controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbricos son inmaduros y se les conoce debilidades;

b) la información almacenada en los computadores móviles pueden no tener backups debido al ancho de banda limitado y/o porque el equipo móvil puede no estar conectado cuando estos backups se realizan.

11.7.2 Teletrabajo

Control

Se deberían desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

Guía de Implementación

Las organizaciones sólo deberían autorizar las actividades de teletrabajo si se han satisfecho las disposiciones y controles de seguridad apropiados y se cumple la política de seguridad de la organización.

Se debería proteger debidamente el lugar de teletrabajo contra, por ejemplo, el robo del equipo o información. La distribución no autorizada de información, el acceso remoto no autorizado a los sistemas internos de la organización o el mal uso de los dispositivos. Es importante, que el teletrabajo se autorice y controle por la gerencia, y que existan los acuerdos adecuados para este tipo de trabajo.

Se debería considerar lo siguiente:

a) la seguridad física real del lugar de teletrabajo, teniendo en cuenta la del edificio y la de su entorno local;

b) el entorno de teletrabajo propuesto;

c) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la criticidad de la información a acceder y el paso por alto del enlace de comunicación y de la criticidad del sistema interno;

d) la amenaza de acceso no autorizado a información y recursos por otras personas próximas, por ejemplo, la familia o amigos;

e) el uso de redes de casa y los requisitos o restricciones de la configuración de los servicios inalámbricos;

f) las políticas y procedimientos para prevenir las disputas concernientes a los derechos de la propiedad intelectual desarrollada en equipos privados propios;

g) el acceso a un equipo privado propio (para verificar la seguridad de la maquina o durante una investigación), que puede ser prevenido por la legislación;

h) los acuerdos de licencia de software que hará que dichas organizaciones se vuelvan confiables para el licenciamiento de software de clientes en las estaciones de trabajo pertenecientes a empleados, contratistas o terceros;

i) la protección antivirus y los requerimientos de firewall.

Los controles y adecuaciones a ser consideradas incluyen:

a) el aprovisionamiento del equipo y mobiliario adecuados para las actividades de teletrabajo, donde no esta permitido el uso de equipos privados propios que no estén bajo el control de la organización;

b) la definición del trabajo permitido, las horas de trabajo, la clasificación de la información que puede utilizar y los sistemas y servicios internos a los que el teletrabajador esté autorizado a acceder;

c) el suministro del equipo de comunicación adecuado, incluidos los métodos para asegurar el acceso remoto;

d) la seguridad física;

e) reglas y guías sobre la familia y el acceso de visitas al equipo y la información;

f) proporcionar el soporte y mantenimiento para el hardware y el software;

g) proporcionar una póliza de seguros;
h) los procedimientos de respaldo y continuidad del negocio;

i) la auditoria y seguimiento de la seguridad;

j) la revocación de autorizaciones, derechos de acceso y devolución del equipo cuando cesen las actividades de teletrabajo.

Otra Información

El teletrabajo utiliza la tecnología de comunicaciones para permitir al personal trabajar remotamente desde una locación ubicada fuera de la organización.

12. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

12.1 Requisitos de seguridad de los sistemas

OBJETIVO: Asegurar que la seguridad esté imbuida dentro de los sistemas de información.

Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar los sistemas de información.

Todos los requisitos de seguridad deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control.

Guía de Implementación

Las especificaciones deberían considerar los controles automatizados a ser incorporados en el sistema y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares cuando se evalúen, desarrollen o compren paquetes de software para aplicaciones de negocio.

Los requisitos y controles de seguridad deberían reflejar el valor de los activos de información implicados (véase el inciso 7.2) y el posible daño a la organización que resultaría de fallos o ausencia de seguridad.

Los requisitos del sistema para la seguridad de información y procesos para implementar la seguridad deben ser integrados en las etapas iniciales de los proyectos de sistema de información. Los controles introducidos en la etapa de diseño son significantemente menos costos de implementar y mantener que los que se incluyen durante o después de la implementación.

Si los productos son comprados, se debe realizar una prueba formal y un proceso de adquisición. Los contratos con el proveedor deben indicar los requisitos de seguridad. Si los requisitos no satisfacen la funcionalidad de la seguridad en un producto se debe reconsiderar los riesgos introducidos y los controles asociados antes de comprar el producto. Donde se suministre una funcionalidad adicional que cause un riesgo en la seguridad, se debe desactivar o se debe revisar la estructura del control propuesto para determinar si se puede tomar ventaja de la funcionalidad disponible.

Otra Información

Si se considera apropiado, por ejemplo por razones de costos, la gerencia puede desear hacer uso de productos independientemente evaluados y certificados. Para mayor información sobre

el criterio de evaluación para productos de seguridad de TI se puede consultar la ISO/IEC 15408 u otro estándar de evaluación o certificación.

La ISO/IEC TR 13335-3 provee guía en el uso de los procesos de gestión de riesgos para identificar los requisitos para controles de seguridad.

12.2 Seguridad de las aplicaciones del sistema

OBJETIVO: Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

Se deberían diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Se podrá requerir controles adicionales para sistemas que procesen o tengan impacto en información sensible, con mucho valor o críticas. Estos controles deben ser determinados en base a los requisitos de seguridad y la evaluación de riesgos.

12.2.1 Validación de los datos de entrada

Control

Se deberían validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas.

Guía de Implementación

Se deberían aplicar verificaciones a la entrada de las transacciones, de los datos de referencia (por ejemplo nombres y direcciones, límites de crédito, números de clientes) y de las tablas de parámetros (por ejemplo precios de venta, tasas de cambio de divisas, tasas de impuestos). Los controles siguientes deberían ser considerados:

a) entrada duplicada u otras verificaciones, como verificación de fronteras o campos limitados para especificar los rangos de los datos de entrada, para detectar los errores siguientes:

l) valores fuera de rango;

2) caracteres inválidos en los campos de datos;

3) datos que faltan o están incompletos;

4) datos que exceden los límites de volumen por exceso o defecto;

5) datos de control no autorizados o inconsistentes;

b) revisión periódica del contenido de los campos clave o los archivos de datos para confirmar su validez e integridad;

c) inspección de los documentos físicos de entrada para ver si hay cambios no autorizados a los datos de entrada (todos deberían estar autorizados);

d) procedimientos para responder a los errores de validación;

e) procedimientos para comprobar la integridad de los datos de entrada;

f) definición de las responsabilidades de todos los implicados en el proceso de entrada de datos;

g) creación de un registro de actividades envueltas en el procesamiento de los datos de entrada (véase el inciso 10.10.1).

Otra Información

La reexaminación automática y la validación de los datos de entrada pueden ser consideradas, donde sea aplicable, para reducir el riesgo de errores y para prevenir los ataques estándar incluyendo el desbordamiento del buffer y la inyección del código.

12.2.2 Control del proceso interno

Control

Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.

Guía de Implementación

El diseño de las aplicaciones debería asegurar la implantación de restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad. Areas de riesgo específicas a considerar serían:

a) el uso en los programas de funciones ‘añadir’ y ‘borrar’ para cambiar los datos;

b) los procedimientos para evitar programas que corran en orden equivocado o después del fallo de un proceso anterior (véase el inciso10.1.1);

c) el uso de programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos;

d) la protección contra ataques utilizando corridas o desbordes de buffers.

Se debería tener preparado una lista de verificación apropiada, tener las actividades documentadas y los resultados deben mantenerse seguros. A continuación se dan ejemplos de comprobaciones que pueden incorporarse:

a) controles de sesión o de lotes, para conciliar los cuadres de los archivos tras las actualizaciones de las transacciones;

b) controles para comprobar los cuadres de apertura contra los cuadres previos del cierre, como:

1) controles de pasada en pasada;

2) totales de actualización de archivos;

3) controles de programa a programa;

c) validación de los datos generados por el sistema (véase el inciso 12.2.1);

d) comprobaciones de la integridad, autenticidad u otro aspecto de seguridad de datos o del software transferidos entre el computador central y las computadoras remotas;

e) totales de comprobación de registros y archivos;

f) comprobaciones que aseguren que los programas de las aplicaciones se ejecutan en el momento adecuado;

g) comprobaciones que aseguren que los programas se ejecutan en el orden correcto, que finalizan en caso de falla y que no sigue el proceso hasta que el problema se resuelve.

h) crear un registro de las actividades envueltas en el procesamiento (véase el inciso 10.10.1).

Otra Información

Los datos que han sido ingresados correctamente pueden ser corrompidos por errores de hardware, procesamiento de errores o a través de actos deliberados. La comprobación requerida dependerá de la naturaleza de la aplicación y del impacto en el negocio de cualquier corrupción de datos.

12.2.3 Integridad de mensajes

Control

Se debería identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se deberían de identificar e implementar controles apropiados.

Guía de Implementación

Una evaluación de riesgos de seguridad debe ser llevada a cabo para determinar si la integridad de los mensajes es requerida e identificar el método mas apropiado para su implementación.

Otra Información

Se pueden usar técnicas criptográficas (véase el inciso 12.3) como un medio adecuado para implantar dicha autenticación.

12.2.4 Validación de los datos de salida

Control

Se deberían validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias.

Guía de Implementación

La validación de salidas puede incluir:

a) validaciones de verosimilitud para comprobar que los datos de salida son razonables;

b) cuentas de control de conciliación para asegurar el proceso de todos los datos;

c) suministro de suficiente información al lector o a un sistema de proceso subsiguiente para poder determinar la exactitud, completitud, precisión y clasificación de la información;

d) procedimientos para contestar los cuestionarios de validación de salidas;

e) definición de las responsabilidades de todos los implicados en el proceso de salida de datos;

f) creación de un registro de actividades en el proceso de validación de los datos de salida.

Otra Información

Típicamente, los sistemas y aplicaciones son construidos con la suposición de que si se tomo en cuenta una validación, verificación y prueba apropiada, las salidas serán siempre correctas. Sin embargo, esta suposición no siempre es valida ya que existen sistemas que han sido probados y que pueden producir aún salidas incorrectas bajo ciertas circunstancias.

12.3 Controles criptográficos

OBJETIVO: Proteger la confidencialidad, autenticidad o integridad de la información.

Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

12.3.1 Política de uso de los controles criptográficos

Control

La organización debería desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información.

Guía de Implementación

El desarrollo de una política debería considerar lo siguiente:

a) un enfoque de gestión del uso de las medidas criptográficas a través de la organización, incluyendo los principios generales en base a los cuales se debería proteger la información del negocio (véase el inciso 5.1.1);

b) basados en la evaluación de riesgos, el nivel requerido de protección debe ser identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido;

c) el uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación;

d) un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves;

e) los roles y responsabilidades de cada cual que es responsable de:

1) la implementación de la política

2) la gestión de claves, incluyendo la generación de claves (véase el inciso 12.3.2);

f) los estándares a ser adoptados para una efectiva implementación a través de la organización (que solución es utilizada para cada proceso del negocio);

g) las normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus).

Cuando se implemente la política criptográfica de la organización se debe tener en consideración las regulaciones y restricciones nacionales que pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los temas de desbordamiento de información fuera de las fronteras (véase el inciso 15.1.6).

Los controles criptográficos pueden se utilizados para alcanzar diferentes objetivos de seguridad como por ejemplo:

a) confidencialidad: utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.
b) integridad/autenticidad: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.

c) no repudio: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

12.3.2 Gestión de claves

Control

La gestión de claves debe criptográficas debe apoyar el uso de las técnicas criptográficas en la organización.

Guía de Implementación

Se deberían proteger todos los tipos de claves de su modificación o destrucción; las claves secretas y las privadas además requieren protección contra su distribución no autorizada. Con este fin también pueden usarse técnicas criptográficas. Se debería utilizar protección física para cubrir el equipo usado en la generación, almacenamiento y archivo de claves.

El sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para distintos sistemas criptográficos y distintas aplicaciones;

b) generar y obtener certificados de clave pública;

c) distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves;

d) almacenar claves, incluyendo la forma de obtención de acceso a las claves por los usuarios;

e) cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse;

f) tratar las claves comprometidas (afectadas);

g) revocar claves, incluyendo la forma de desactivarlas o retirarlas, por ejemplo, cuando tienen problemas o el usuario deja la organización (en cuyo caso las claves también se archivan);

h) recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio, por ejemplo, para recuperar la información cifrada;

i) archivar claves, por ejemplo, para información archivada o de respaldo;

j) destruir claves;

k) hacer seguimiento y auditorias de las actividades relacionadas con la gestión de las claves.

Para reducir la probabilidad de comprometer las claves, se deberían definir fechas de activación y desactivación para que sólo puedan utilizarse durante un periodo limitado. Este debería depender de las circunstancias del uso de las medidas de control criptográficas y del riesgo percibido.
Además de la gestión segura de las claves privadas y secretas, se debería considerar la autenticidad de las claves públicas. Este proceso se realiza normalmente por una autoridad certificadora que debería ser una organización reconocida y poseer controles y procedimientos adecuados para proporcionar el grado de fiabilidad requerido.

El contenido de los acuerdos de nivel de servicio o de los contratos con los proveedores de servicios criptográficos (por ejemplo una autoridad certificadora) debería cubrir los aspectos de las obligaciones, fiabilidad de los servicios y tiempos de respuesta para su suministro (véase el inciso 6.2.3).

Otra Información

La gestión de claves criptográficas es esencial para un uso efectivo de las técnicas criptográficas. La ISO/IEC 11770 provee mayor información de la gestión de claves. Los dos tipos de técnicas criptográficas son:

a) las técnicas de clave secreta, donde dos o más partes comparten la misma clave, que se usa tanto para cifrar como para descifrar la información. Este clave ha de mantenerse en secreto, puesto que cualquiera que acceda a ella puede descifrar la información cifrada o introducir información no autorizada;

b) las técnicas de clave pública, donde cada usuario tiene un par de claves, una pública (que puede conocer cualquiera) y otra privada (que ha de mantenerse en secreto). Estas técnicas se usan para cifrado y para producir firmas digitales (véase también ISO/IEC 9796 y la ISO/IEC 14888).

Existe una amenaza en forjar una firma digital reemplazando una clave pública de usuario. Este problema es traído por el uso de un certificado clave público.

Las técnicas criptográficas pueden ser utilizadas para proteger claves criptográficas. Los procedimientos pueden necesitar ser considerados para maniobrar pedidos legales de acceso a las claves criptográficas, por ejemplo la información cifrada puede necesitar ser disponible de una manera no cifrada como evidencia en un caso de corte.

12.4 Seguridad de los archivos del sistema

OBJETIVO: Asegurar la seguridad de los archivos del sistema.

El acceso a los archivos del sistema debería ser controlado y los proyectos de Tecnología de la Información (TI) y las actividades complementarias deben ser llevadas a cabo de una forma segura. Se debería tener cuidado de evitar la exposición de datos sensibles en ambientes de prueba.

12.4.1 Control del software en producción

Control

Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.

Guía de Implementación

Para minimizar el riesgo de corrupción deberían considerarse los siguientes controles:

a) la actualización de las librerías de programas operativos sólo se debería realizar por el administrador capacitado previa autorización de la gerencia (véase el inciso 12.4.3);

b) los sistemas operativos deberían tener sólo código ejecutable y no desarrollo de código o compiladores;

c) no se debería implantar código ejecutable en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuente. Deben ser realizadas en un sistema separado (véase el inciso 10.1.4);

d) se debería utilizar un sistema de control de configuración para mantener un control de todo el software implementado así como la documentación del sistema;

e) debería existir una estrategia de restauración no actualizada antes de que se implementen los cambios;

f) se debería mantener un registro de auditoria de todas las actualizaciones a las librerías de programas en producción;

g) se deberían retener las versiones anteriores de software como medida de precaución para contingencias;

h) las versiones antiguas de software deben ser archivadas junto con toda la información requerida, los parámetros, procedimientos, detalles de configuración y software de soporte, durante el tiempo en que los datos sean retenidos.

El software adquirido que se use en sistemas operativos se debería mantener en el nivel de soporte del proveedor. A través del tiempo, los vendedores de software cesaran de suministrar versiones antiguas. La organización debe considerar los riesgos de confiar en un software que no cuente con soporte.

Cualquier decisión de actualización debe tomar en cuenta los requisitos del negocio para dicho cambio y la seguridad del nuevo lanzamiento, como por ejemplo la introducción de una nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión. Los parches de software deben ser aplicados cuando ayuden a remover o reducir las vulnerabilidades (véase el inciso 12.6.1).

Sólo se debería permitir acceso físico o lógico a los proveedores cuando sea imprescindible por motivos de soporte, y con aprobación de la gerencia. Las actividades de los proveedores deberían ser supervisadas y controladas.
El software de computación debe recaer en software y módulos suministrados externamente los cuales deben ser monitoreados y controlados para evitar cambios no autorizados que puedan introducir debilidades en la seguridad.

Otra Información

Los sistemas operativos solo deben ser actualizados cuando exista un requerimiento para realizarlo, por ejemplo si la versión actual no apoya los requerimientos del negocio. Las actualizaciones no deben realizarse solo porque exista una nueva versión disponible. Las nuevas versiones de sistemas operativos pueden ser menos seguras, menos estables y menos entendibles que la versión actual.

12.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.

Guía de Implementación

Se debería evitar el utilizar bases de datos en producción que contengan información de personas. Si esta información se utilizase, los datos personales se deberían modificar o remover antes de utilizarlos para las pruebas. Se deberían aplicar los controles y medidas siguientes para proteger los datos de producción cuando se usen para pruebas:

a) los procedimientos de control de acceso que se consideran para las aplicaciones del sistema operacional se deberían utilizar también en los sistemas de aplicaciones en prueba;

b) se debería autorizar por separado cada vez que se copie información operativa a un sistema de aplicación en prueba;

c) se debería borrar la información operativa de la aplicación del sistema en prueba en cuanto ésta se complete;

d) se debería registrar la copia y uso de la información operativa a efectos de seguimiento para auditoria.

Otra Información

Los sistemas de prueba usualmente requieren de volúmenes substanciales de datos de prueba que sean lo más parecidos a los datos operacionales.

12.4.3 Control de acceso a los códigos de programas fuente

Control

El acceso a los códigos de programas fuente debe ser restringido.

Guía de Implementación

El acceso a los programas de códigos fuente y sus ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) deben ser controlados estrictamente con el fin de prevenir la introducción de funcionalidades no autorizadas y para evitar los cambios no intencionales. Para los códigos de programas fuente, esto puede ser logrado, controlando el almacenaje central de dicha fuente, preferentemente en librerías de programas fuente. Las siguientes pautas deben ser consideradas (véase también el capitulo 11) para controlar el acceso a dicha librería de programas fuente, con el fin de reducir la probabilidad de corrupción de los programas del sistema.

a) si es posible, las librerías de programas fuentes no deberían residir en los sistemas operativos;

b) el código y librería de programas fuente debe ser maniobrado de acuerdo a procedimientos establecidos;

c) el personal de apoyo informático no debería tener libre acceso, sin restricción, a las librerías de programas fuentes;

d) la actualización de librerías de programas y la entrega de programas a los programadores se debería realizar sólo por el responsable con autorización del gerente de soporte informático para la aplicación;

e) los listados de programas se deberían mantener en un entorno seguro (véase el inciso10.7.4);

f) se debería mantener un registro de auditoria de todos los accesos a las librerías de programas fuentes;

g) el mantenimiento y copia de las librerías de programas fuente debería estar sujeta a procedimientos estrictos de control de cambios (véase el inciso 12.5.1).

Otra Información

Los códigos de programas fuente son códigos realizados por programadores los cuales son compilados para crear ejecutables. Ciertos lenguajes de programación no distinguen formalmente el código fuente con los ejecutables ya que estos ejecutables son creados cuando estos son activados.

Los estándares ISO 10007 e ISO/IEC 122207 proveen mayor información sobre la gestión de configuración y el proceso ciclo de vida del software.

12.5 Seguridad en los procesos de desarrollo y soporte

OBJETIVO: Mantener la seguridad del software de aplicación y la información.

Se deberían controlar estrictamente los entornos del proyecto y de soporte.

Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

12.5.1 Procedimientos de control de cambios

Control

La implementación de cambios debe ser controlada usando procedimientos formales de cambio.

Guía de Implementación

Para minimizar la corrupción de los sistemas de información, se deberían mantener estrictos controles sobre la implantación de cambios. La introducción de nuevos sistemas y cambios mayores al sistema existente debe seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación.

Este proceso debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios. Este proceso debe también asegurar que no se comprometa la seguridad y los procedimientos de control existentes, que a los programadores de soporte se les de acceso solo a las partes del sistema necesarias para su trabajo y que se debe tener una aprobación y acuerdo formal para cualquier cambio.

La aplicación y sus procedimientos de control de cambios deberían estar integrados siempre que sea posible (véase el inciso 10.1.2). Este proceso debería incluir:

a) el mantenimiento de un registro de los niveles de autorización acordados;

b) la garantía de que los cambios se realizan por usuarios autorizados;

c) la revisión de los controles y los procedimientos de integridad para asegurarse que los cambios no los debilitan;

d) la identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora;

e) la obtención de la aprobación formal para propuestas detalladas antes de empezar el trabajo;

f) la garantía de la aceptación por el usuario autorizado de los cambios antes de cualquier implantación;

g) la garantía de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua;

h) el mantenimiento de un control de versiones de toda actualización del software;

i) el mantenimiento de un seguimiento de auditoria de todas las peticiones de cambio;

j) la garantía del cambio de la documentación operativa (véase el inciso 10.1.1) y de los procedimientos de usuario en función de la necesidad;

k) la garantía de la adecuación del tiempo de implantación de los cambios para no dificultar los procesos de negocio implicados.

Otra Información

Los cambios en el software pueden impactar en el ambiente operacional.

Las buenas practicas incluyen la prueba de nuevo software en un ambiente segregado de los ambientes de producción y desarrollo (véase el inciso 10.1.4). Esto permite controlar el nuevo software y aumentar la protección de la información operativa que se use para pruebas. Se deben incluir parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automáticas no deben ser utilizadas en sistemas críticos ya que algunas actualizaciones pueden causar que las aplicaciones criticas fallen (véase el inciso 12.6).

12.5.2 Revisión técnica de los cambios en el sistema operativo

Control

Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.

Guía de Implementación

Este proceso debería cubrir:

a) la revisión de los procedimientos de control de la aplicación y de la integridad para asegurar que los cambios en el sistema operativo no han sido comprometidos;

b) la garantía de que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema que requieran los cambios del sistema operativo;

c) la garantía de que la modificación de los cambios del sistema operativo se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación;

d) la garantía de que se realizan los cambios apropiados en los planes de continuidad del negocio (véase el capítulo 14).

Se le debe dar la responsabilidad, a un grupo específico o individuo, de monitorear las vulnerabilidades y los lanzamientos de parches y arreglos por parte de los vendedores (véase el inciso 12.6).

12.5.3 Restricciones en los cambios a los paquetes de software

Control

No se recomiendan modificaciones a los paquetes de software. Se debería limitar a cambios necesarios y todos estos deben ser estrictamente controlados.

Guía de Implementación

Se deberían usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable. Cuando haya necesidad de modificarlos, se deberían considerar los aspectos siguientes:

a) el riesgo de debilitamiento de las medidas de control incorporadas y sus procesos de integridad;

b) la obtención del consentimiento del vendedor;

c) la posibilidad de obtener los cambios requeridos como actualizaciones normales del programa del vendedor;

d) el impacto causado si la organización adquiere la responsabilidad del mantenimiento futuro del software como resultado de los cambios.

Si se considera que son necesarios los cambios, se debería guardar el software original y los cambios realizados en una copia claramente identificada. Un proceso de gestión de actualización de software debe ser implementado para asegurar que exista la mayor cantidad de parches actuales y de actualizaciones instaladas para todo el software autorizado (véase 12.6). Se deberían probar y documentar totalmente los cambios de forma que puedan volverse a aplicar a las actualizaciones del software. Si fuese necesario, las modificaciones pueden ser probadas y validadas por un cuerpo independiente de evaluación.

12.5.4 Fuga de Información

Control

Las oportunidades de fuga de información deben ser prevenidas.

Guía de Implementación

Se debe considerar lo siguiente para limitar el riesgo de fuga de información, como por ejemplo a través del uso y explotación de canales cubiertos:

a) escaneo de medios de salida y comunicaciones para información oculta;

b) sistema de modulación y enmascarado, y el comportamiento de las comunicaciones para reducir la probabilidad de que un tercero sea capaz de deducir información desde dicho comportamiento;

c) haciendo uso de los sistemas y software que se consideran de alta integridad, por ejemplo productos evaluados (véase ISO/IEC 15408);

d) monitoreo regular de las actividades del personal y del sistema, donde sea permitido bajo la legislación o regulación existente;

e) monitoreo del uso de recursos en sistemas de cómputo.

Otra Información

Un canal encubierto son trayectorias que no tienen previsto conducir información, pero que sin embargo pueden existir en un sistema o red. Por ejemplo, la manipulación de bits en paquetes de protocolos de comunicación puede ser utilizada como un método oculto de señalar. Debido a su naturaleza, prevenir la existencia de todos los canales cubiertos posibles seria muy difícil, si no es imposible. De todas formas, la explotación de dichos canales es realizado frecuentemente por código Troyano (véase también 10.4.1). Tomando medidas para protegernos contra códigos troyanos, reduce el riesgo de la explotación del canal cubierto.

La prevención de acceso a red no autorizado (véase el inciso 11.4), así como las políticas o procedimientos para que desaliente el mal uso de los servicios de información por parte del personal (véase el inciso 15.1.5), ayudara a protegernos contra canales cubiertos.

12.5.5 Desarrollo externo del software

Control

El desarrollo externo del software debe ser supervisado y monitoreado por la organización.

Guía de Implementación

Deberían ser considerados los siguientes aspectos cuando se externalice el desarrollo de software:

a) acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual (véase el inciso 15.1.2);

b) certificación de la calidad y exactitud del trabajo realizado;

c) acuerdos para hacerse cargo en el caso de fallo de terceros;

d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado;

e) requisitos contractuales sobre la calidad y funcionalidad segura del código;

f) pruebas antes de la implantación para detectar el código Troyano.

12.6 Gestión de la vulnerabilidad técnica

OBJETIVO: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica debe ser implementada de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad. Estas consideraciones deben incluir los sistemas operativos y otras aplicaciones en uso.

12.6.1 Control de las vulnerabilidades técnicas.

Control

Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar a los riegos asociados.

Guía de Implementación

Un inventario actual y completo de activos (véase el inciso 7.1) es un prerrequisito para una efectiva gestión de vulnerabilidades técnicas. La información especifica requerida para apoyar la gestión de vulnerabilidades técnicas incluye al vendedor de software, numero de versiones, el estado actual de despliegue (por ejemplo que software es instalado en que sistema) y las personas dentro de la organización responsables del software.

Una acción apropiada y a tiempo debe ser tomada en cuenta en respuesta a la identificación de vulnerabilidades técnicas potenciales. Las siguientes pautas deben seguirse para establecer un proceso de gestión de vulnerabilidades técnicas efectivas:

a) la organización debe definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquier otra responsabilidades coordinadas;

b) los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre ellos se deben identificar para el software y otras tecnologías (basadas en el inventario de activos, véase 7.1.1); estos recursos de información deben ser actualizados basados en cambios de inventario o cuando un recurso nuevo o mas útil se encuentre;

c) se debería definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes;

d) una vez identificada las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Esta acción puede implicar el parchado de sistemas vulnerables y/o la aplicación de otros controles;

e) dependiendo en que tan urgente sea necesario tratar una vulnerabilidad técnica, la acción a ser tomada en cuenta debe ser llevada a cabo de acuerdo a controles relacionados con la gestión de cambios (véase el inciso 12.5.1) o siguiendo los procedimientos de respuesta ante incidentes en la seguridad de información (véase el inciso 13.2);

f) si un parche se encuentra disponible, se deben tratar los riesgos asociados con la instalación (los riesgos planteados por la vulnerabilidad deben ser comparados con los riesgos de instalación del parche);

g) los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos y que no resulten en efectos secundarios que no puedan ser tolerados; si no existe ningún parche disponible, se deberían considerar otros controles como:

1) apagar los servicios y capacidades relacionadas con la vulnerabilidad;
2) adaptar o tratar los controles de acceso, por ejemplo los firewall en los bordes de red (véase el inciso 11.4.5);

3) monitoreo creciente para detectar o prevenir ataques actuales;

4) aumento en la precaución de la vulnerabilidad;

h) un registro de ingreso debe ser mantenido para todos los procedimientos emprendidos;

i) se debería monitorear y evaluar la gestión de procesos en la vulnerabilidad técnica con el fin de asegurar su efectividad y eficiencia;

j) los sistemas en alto riego deben ser tratados primero.

Otra Información

El funcionamiento correcto de un proceso de gestión de vulnerabilidades técnicas de una organización es crítico para muchas organizaciones y por lo tanto debe ser monitoreado. Un

inventario actualizado es esencial para asegurar que las vulnerabilidades técnicas potenciales sean identificadas.

La gestión de vulnerabilidades técnicas puede ser vistas como una sub-función de la gestión de cambios y puede tomar ventaja de los procesos y procedimientos de la gestión de cambios (véase 10.1.2 y 12.5.1).

Los vendedores se encuentran frecuentemente bajo una presión significante para lanzar los parches lo más rápido posible. Es por este motivo que los parches pueden no tratar el problema adecuadamente trayendo consigo efectos secundarios negativos. Igualmente, en algunos casos, desinstalar el parche puede ser difícil de realizar una vez que este se ha aplicado.

Si no es posible una prueba adecuada de los parches debido al costo o a la falta de recursos, se puede considerar una demora en el parchado para evaluar los riesgos asociados, basándonos en la experiencia reportada por otros usuarios.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

13.1 Reportando eventos y debilidades de la seguridad de información

OBJETIVO: Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

El reporte formal de eventos y los procedimientos de escalada deben estar implementados. Todos los empleados, contratistas y terceros deben estar al tanto de los procedimientos para reportar los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales. Se les debe requerir que reporten cualquier evento o debilidad en la seguridad de información, lo más rápido posible, al punto de contacto designado.

13.1.1 Reportando los eventos en la seguridad de información

Control

Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada

Guía de Implementación

Un procedimiento formal de reporte de eventos en la seguridad de información debe ser establecido junto con una respuesta a incidencias y procedimientos de escalada, estableciendo las acciones a ser tomadas en cuenta al recibir dicho reporte. Se debe establecer un punto de contacto para el reporte de eventos en la seguridad de información. Se debe asegurar que este punto de contacto es conocido a través de la organización, este siempre disponible y que sea capaz de proveer una respuestas adecuada y a tiempo.

Todos los empleados, contratistas y terceros deben ser prevenidos sobre sus responsabilidades de reportar cualquier evento en la seguridad de información lo más rápido posible. Igualmente, deben ser prevenidos del procedimiento para reportar dicho evento y del punto de contacto. Los procedimientos de reporte deben incluir:

a) procesos de retroalimentación adecuados para asegurar que dichos eventos reportados de la seguridad de información sean notificados de los resultados después de que el tema haya sido repartido y cerrado;

b) formularios de reporte de eventos en la seguridad de información, con el fin de apoyar la acción de reporte y para ayudar a la persona que reporta recordar todas las acciones necesarias en caso de un evento;

c) el comportamiento correcto a ser emprendido en caso de un evento en la seguridad de información, por ejemplo:

1) notar todos los detalles importantes (tipos de no conformidad, mal funcionamiento, aberturas, mensajes en la pantalla, conducta extraña) inmediatamente;

2) no llevar a cabo ninguna acción por si mismo, pero reportar inmediatamente al punto de contacto;

d) referencias a un proceso formal disciplinario establecido para tratar con empelados, contratistas o terceros que cometan una abertura en la seguridad.

En ambientes de alto riesgo, se debe proveer una alarma de obligación con el que una persona pueda indicar dichos problemas. Los procedimientos para responder a las alarmas de obligación deben reflejar la situación de alto riesgo que las alarmas están indicando.

Otra Información

Ejemplos de eventos e incidentes en la seguridad de información son:

a) perdida de servicio, equipo o instalaciones;

b) sobrecargo o mal funcionamiento del sistema;

c) errores humanos;

d) no conformidades con políticas o pautas;

e) aberturas en los arreglos de seguridad física;

f) cambios incontrolables en el sistema;

g) mal funcionamiento del software o hardware;

h) violación de acceso.

Teniendo el debido cuidado en aspectos de confidencialidad, los incidentes en la seguridad de información puede ser utilizado en el entrenamiento de prevención de usuarios (véase el inciso 8.2.2) como ejemplo de lo que podría suceder, como responder a tales incidentes y como evitarlos en un futuro. Para ser capaz de tratar propiamente eventos e incidentes de la seguridad de información puede ser necesario recolectar evidencia lo mas pronto posible después de la ocurrencia (véase el inciso 13.2.3).

El mal funcionamiento u otro comportamiento anormal en el sistema puede ser un indicador de un ataque de seguridad o de una abertura en la seguridad y debe ser siempre reportado como un evento de la seguridad de información.

Para mayor información sobre el reporte de eventos y la gestión de incidentes en la seguridad de información se puede consultar la ISO/IEC TR 18044.

13.1.2 Reportando debilidades en la seguridad de información

Control

Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.

Guía de Implementación

Todos los empleados, contratistas y terceros deben reportar estas materias a sus gerencias o directamente al proveedor del servicio lo más pronto posible con el fin de prevenir los incidentes en la seguridad de información. El mecanismo de reporte debe ser fácil, accesible y disponible como sea posible. Deben ser informados que por ninguna circunstancia deben tratar de probar una debilidad sospechosa.

Otra Información

Los empleados, contratistas y terceros deben ser advertidos a no tratar de probar debilidades de seguridad sospechosas. Probar las debilidades puede ser interpretado como un potencial mal uso del sistema y puede ocasionar daño al sistema o servicio de información y resultar en responsabilidad legal para el individuo que realiza la prueba.

13.2 Gestión de las mejoras e incidentes en la seguridad de información

OBJETIVO: Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de información.

Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados. Un proceso de mejora continua debe ser aplicado en respuesta al monitoreo, evaluación y gestión general de los incidentes en la seguridad de información.

Donde se requiera evidencia, esta debe ser recolectada para asegurar el cumplimiento de los requisitos legales.

13.2.1 Responsabilidades y procedimientos

Control

Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.

Guía de Implementación

En adición a los reportes de eventos y debilidades en la seguridad de información (véase el inciso 13.1), el monitoreo de los sistemas, alertas y vulnerabilidades (véase el inciso 10.10.2), deben ser utilizados para detectar los incidentes en la seguridad de información. Las siguientes pautas deben ser consideradas para los procedimientos en la gestión de incidentes en la seguridad de información:

a) los procedimientos deben ser establecidos para maniobrar diferentes tipos de incidentes en la seguridad de información como por ejemplo:

1) fallas y perdidas de servicio en los sistemas de información;

2) código malicioso (véase el inciso 10.4.1);

3) negación de servicio;

4) errores resultantes de datos incompletos o no actualizados;

5) aperturas en la confidencialidad e integridad;
6) mal uso de los sistemas de información;

b) en adición a los planes de contingencias normales (véase el inciso 14.1.3), los procedimientos también deben cubrir (véase el inciso 13.2.2):

1) análisis e identificación de la causa del incidente;

2) contención;

3) si es necesario, planeamiento e implementación de acciones correctivas para prevenir la re ocurrencia;

4) comunicaciones con lo afectados o implicados en recuperarse del incidente;

5) reportar acciones a la autoridad apropiada;

c) un registro de auditorias y se debe recolectar evidencia similar (véase el inciso 13.2.3) y resguardada como sea apropiado para:

1) análisis de problemas internos;

2) el uso de evidencia forense en relación con una apertura potencial del contrato, requisitos regulados o en el caso de procedimientos civiles o criminales, como por ejemplo el mal uso del computador o la legislación de protección de datos;

3) negociaciones para compensaciones por parte de los proveedores de software o del servicio;

d) acción para recuperarse de aperturas de seguridad y controlar formal y cuidadosamente las fallas del sistema que han sido corregidas; los procedimientos deben asegurar que:

1) solo el personal claramente identificado y autorizado están permitidos de acceder a los sistemas y datos vivos (véase también 6.2 para acceso externo);

2) todas las acciones de emergencia que se realizaron sean documentadas a detalle;

3) las acciones de emergencia sean reportadas a la gerencia y revisados de una manera ordenada;

4) la integridad de los sistemas y controles de negocio son confirmados con un mínimo de retraso.

Los objetivos de la gestión de incidentes en la seguridad de información deben estar acorde con la gerencia y se debe asegurar que los responsables para la gestión entienden las prioridades de la organización para maniobrar dichos incidentes.

Otra Información

Los incidentes en la seguridad de información pueden trascender las barreras organizacionales y nacionales. Para responder a dichos incidentes existe una creciente necesidad de coordinar respuestas y de compartir información con organizaciones externas como sea apropiado.

13.2.2 Aprendiendo de los incidentes en la seguridad de información

Control

Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.

Guía de Implementación

La información ganada de la evaluación de los incidentes en la seguridad de información deben ser utilizados para identificar incidentes que se repiten o de gran impacto.

Otra Información

La evaluación de los incidentes en la seguridad de información puede indicar la necesidad de controles realzados o adicionales para limitar la frecuencia, daño y costos de ocurrencias futuras o para ser tomado en cuenta en el proceso de revisión de la política de seguridad (véase el inciso 5.1.2).

13.2.3 Recolección de evidencia

Control

Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.

Guía de Implementación

Los procesos internos deben ser desarrollados y seguidos cuando se recolecte y presente evidencia para propósitos disciplinarios maniobrados dentro de la organización.

En general, las reglas para evidencia cubren:

a) admisibilidad de evidencia: si es que la evidencia puede ser utilizada en corte;

b) peso en la evidencia: calidad y lo completo de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debe asegurar que sus sistemas de información cumplen con cualquier estándar o código publicado de práctica para la producción de evidencia admisible.

El peso en la evidencia debe cumplir con cualquier requerimiento aplicable. Para lograr peso en la evidencia, la calidad y lo completo de los controles usados para corregir y proteger consistentemente la evidencia (como por ejemplo el proceso de control de evidencia) durante el periodo en que la evidencia que se recupera se almacena y se procesa, debe estar demostrado por un fuerte seguimiento de dicha evidencia. En general, dicho seguimiento puede ser establecido bajo las siguientes condiciones:

a) para documentos en papel: el original es guardado con seguridad con un registro del individuo que encontró el documento, donde se encontró, cuando fue encontrado y quien presenció dicho descubrimiento. Cualquier investigación debe asegurar que los originales no hayan sido forzados;

b) para información en medios informáticos: se deben de tomar en cuenta imágenes espejo o copias (dependiendo de los requerimientos aplicables) de cualquier medio removible, información en discos duros o en memoria con el fin de asegurar la disponibilidad. El registro de todas las acciones durante el proceso de copiado debe ser mantenido y el proceso debe ser presenciado; el medio original y el registro (si este no es posible, al menos con imágenes espejo o copias) debe ser mantenido de una forma segura e intocable.

Cualquier trabajo forense debe ser realizado solamente en las copias del material en evidencia. La integridad de todo el material en evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizó dichas actividades y que herramientas y programas se utilizaron.

Otra Información

Cuando se detecta un evento en la seguridad de información, no será obvio si es que el evento resultará en corte. Por lo tanto, el peligro requiere que la evidencia necesaria sea destruida intencional o accidentalmente antes de que lo severo del incidente sea realizado. Es recomendable implicar con anticipación a un abogado o a policía ante cualquier acción legal contemplada y tomar consejo en la evidencia requerida.

La evidencia puede trascender las fronteras organizacionales y/o jurisdiccionales. En dichos casos, se debe asegurar que la organización se dedique a recolectar la información requerida como evidencia. Los requerimientos de diferentes jurisdicciones deben ser también considerados para maximizar las oportunidades de admisión a través de las jurisdicciones relevantes.

14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de la gestión de continuidad del negocio

OBJETIVO: Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.

Se debería implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio. Se deberían desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización.

La gestión de la continuidad del negocio debería incluir en adición al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales.

14.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio

Control

Se debería instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio a través de la organización que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio.

Guía de Implementación

El proceso debería reunir los siguientes elementos clave de la gestión de continuidad del negocio:

a) comprender los riesgos que la organización corre desde el punto de vista de su vulnerabilidad e impacto, incluyendo la identificación y priorización de los procesos críticos del negocio (véase el inciso 14.1.2);

b) identificar todos los activos implicados en los procesos críticos de negocio (véase el inciso 7.1.1);

c) comprender el impacto que tendrían las interrupciones en el negocio (es importante encontrar soluciones que manejen las pequeñas incidencias así como los grandes accidentes que puedan amenazar la viabilidad de la organización) y establecer los objetivos del negocio en lo referente a los medios informáticos;

d) considerar la adquisición de los seguros adecuados que formarán parte del proceso general de continuidad del negocio así como parte de la gestión operacional de riesgo;

e) identificar y considerar la implementación de controles adicionales de prevención;

f) identificar los recursos financieros, organizacionales, técnicos y ambientales necesarios para que realizar los requisitos identificados de seguridad de información;

g) asegurar la seguridad del personal y la protección de las instalaciones de procesamiento y de la propiedad de la organización;

h) formular y documentar planes de continuidad del negocio, tratando los requisitos de la seguridad de información, en línea con la estrategia acordada (véase el inciso 14.1.3);
i) probar y actualizar regularmente los planes y procesos instalados (véase el inciso 14.1.5);

j) asegurar que la gestión de la continuidad del negocio se incorpora en los procesos y estructura de la organización. Se debería asignar la responsabilidad de coordinar este proceso de gestión a un nivel alto de la organización (véase el inciso 6.1.1).

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

Guía de Implementación

El estudio para la continuidad del negocio debería empezar por la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de negocio, por ejemplo, una falla del equipo, una inundación o un incendio. Se debería

continuar con una evaluación del riesgo para determinar la probabilidad e impacto de dichas interrupciones (en términos tanto de escala de daños como de periodo de recuperación).

La evaluación del riesgo de continuidad de negocio debe ser llevada a cabo con una total implicancia por parte de los propietarios de los recursos y procesos de negocio. Debería considerar todos los procesos del negocio sin limitarse a los dispositivos informáticos, pero debe incluir los resultados específicos para la seguridad de información. Es importante vincular los diferentes aspectos de riesgos para obtener una figura completa de los requerimientos de continuidad de negocio de la organización. La evaluación debe identificar, cuantificar y priorizar los riesgos contra criterios y objetivos relevantes para la organización incluyendo recursos críticos, impactos de las interrupciones, tiempos permisibles de interrupción y prioridades de recuperación.

Se debería desarrollar un plan estratégico para determinar un enfoque global de la continuidad del negocio a partir de los resultados de la evaluación del riesgo. Una vez creada la estrategia, la gerencia deberá respaldarla y crear un plan para implementar dicha estrategia.

14.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información

Control

Se deberían desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos.

Guía de Implementación

El proceso de planificación de la continuidad del negocio debería considerar los siguientes aspectos:

a) la identificación de los procedimientos de emergencia y los acuerdos de todas las responsabilidades;

b) la identificación de las pérdidas aceptables de información y servicios;

c) la implementación de procedimientos que permiten la recuperación y restauración de las operaciones de negocio y la disponibilidad de información en escalas de tiempo requerido. Se necesita particular atención para la evaluación de las dependencias de negocio externas e internas y de los contratos vigentes;

d) los procedimientos operacionales de seguimiento para completar la restauración y recuperación;

e) la documentación de los procedimientos y procesos acordados;

d) la formación apropiada del personal en los procedimientos y procesos de emergencia acordados, incluyendo la gestión de crisis;

e) la prueba y actualización de los planes.

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo, en la recuperación de servicios específicos a los clientes en un plazo aceptable. Se deberían considerar los servicios y recursos necesarios para conseguirlo, incluyendo el personal, los recursos no informáticos y los contratos de respaldo de los dispositivos informáticos. Estos contratos pueden incluir arreglos con terceros en la forma de acuerdos recíprocos o servicios de subscripciones comerciales.

Lo planes de continuidad del negocio deben tratar las vulnerabilidades organizacionales y por lo tanto deben contener información sensible que necesita ser protegida apropiadamente. Las copias de los planes de continuidad del negocio deben ser guardadas en una locación remota, a una distancia suficiente para escapar de cualquier daño de un desastre en el sitio principal. La gerencia debe asegurar que las copias de los planes de continuidad de negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicada al sitio principal. Otro material necesario para ejecutar los planes e continuidad debe ser también almacenado en la locación remota.

Si se utilizan locaciones alternativas temporales, el nivel de control de seguridad implementado debe ser equivalente al sitio principal.

Otra Información

Se debe notar que los planes y actividades de gestión de crisis (véase el inciso 14.1.3 f) deben ser diferentes de la gestión de negocio continua, ya que puede ocurrir una crisis que pueda ser sobrellevada por procedimientos normales de gestión.

14.1.4 Marco de planificación para la continuidad del negocio

Control

Se debería mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.

Guía de Implementación

Cada plan de continuidad del negocio debería describir el alcance para la continuidad, por ejemplo el alcance para asegurar la seguridad y disponibilidad de la información o de los sistemas de información. También debe especificar claramente las condiciones para su activación, así como las personas responsables de ejecutar cada etapa del plan. Cuando se identifiquen nuevos requisitos se deberían corregir de forma apropiada los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los contratos de respaldo existentes. Los procedimientos deben ser incluidos dentro del programa de gestión de cambios de la organización con el fin de asegurar que los temas de la continuidad del negocio sean tratados apropiadamente.

Cada plan debería tener un propietario. Los procedimientos de emergencia y los planes de respaldo manual y de reanudación deberían estar bajo la responsabilidad de los propietarios de los correspondientes recursos o procesos del negocio implicados. Los acuerdos de respaldo por servicios técnicos alternativos -tales como dispositivos informáticos y de comunicaciones- deberían normalmente estar bajo la responsabilidad de los proveedores del servicio.

El marco de planificación para la continuidad del negocio debería considerar lo siguiente:

a) las condiciones para activar los planes que describen el proceso a seguir antes de dicha activación (cómo evaluar la situación, quiénes tienen que estar implicados, etc.);

b) los procedimientos de emergencia que describen las acciones a realizar tras una contingencia que amenace las operaciones del negocio;

c) los procedimientos de respaldo que describen las acciones a realizar para desplazar de forma temporal a lugares alternativos las actividades esenciales del negocio o soportar servicios y para devolver la operatividad a los procesos del negocio en el plazo requerido;

d) procedimientos temporales de operación para seguir con las terminaciones pendientes de reanudación y restauración;

e) los procedimientos de reanudación que describen las acciones a realizar para que las operaciones del negocio vuelvan a la normalidad;

f) un calendario de mantenimiento que especifique cómo y cuándo se harán pruebas del plan, así como el proceso para su mantenimiento;

g) actividades de concientización y formación diseñadas para comprender los procesos de continuidad del negocio y asegurar que los procesos prosigan con eficacia;

h) las responsabilidades de las personas, describiendo a cada responsable de la ejecución de cada etapa del plan. Si se requiere se debería nombrar suplentes;

i) los activos y recursos críticos necesarios para poder realizar los procedimientos de emergencia, respaldo y reactivación.

14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

Control

Los planes de continuidad del negocio se deberían probar regularmente para asegurarse de su actualización y eficacia.

Guía de Implementación

Las pruebas de los planes de continuidad del negocio deben asegurar que todos los miembros del equipo de recuperación y otro personal relevante están prevenidos de los planes y de sus responsabilidades para la continuidad del negocio y la seguridad de información. Todos deben saber su rol cuando el plan sea invocado.

El calendario de pruebas para plan(es) de continuidad del negocio debería indicar cómo y cuándo probar cada elemento del plan. Se recomienda probar los componentes individuales del plan con frecuencia.

Deberían utilizarse diversas técnicas para proporcionar la seguridad de que los planes funcionarán en la vida real. Éstas deberían incluir:

a) la prueba sobre el papel de varios escenarios (analizando las disposiciones de recuperación del negocio con ayuda de ejemplos de interrupciones);

b) las simulaciones (en particular para entrenar en sus respectivos papeles al personal que gestione la crisis tras la contingencia);

c) las pruebas de recuperación técnica (asegurando que los sistemas de información pueden restaurarse con efectividad);

d) las pruebas de recuperación en un lugar alternativo (haciendo funcionar los procesos del negocio en paralelo con las operaciones de recuperación fuera del lugar principal);

e) las pruebas de los recursos y servicios del proveedor (asegurando que los servicios externos proporcionados cumplen el compromiso contraído);

f) los ensayos completos (probando que pueden hacer frente a las interrupciones de la organización, el personal, los recursos y los procesos).

Cualquier organización puede usar estas técnicas, y deberían, en cualquier caso, reflejar la naturaleza del plan de recuperación específico. Los resultados de las pruebas deben ser grabados y las acciones tomadas en cuenta, cuando sea necesario, para mejorar los planes.

Se deberían asignar responsabilidades para revisar regularmente cada plan de continuidad del negocio. Se debería hacer una actualización apropiada del plan tras la identificación de cambios en las características del negocio no reflejadas en los planes de continuidad del negocio. Este proceso formal de control de cambios debería asegurar que las revisiones regulares del plan completo ayuden a reforzar y distribuir los planes actualizados.

Ejemplos de situaciones que necesitarían la actualización de planes: la adquisición de nuevos equipos o la mejora de los sistemas operativos con cambios en:

a) el personal;

b) las direcciones o números de teléfono;

c) la estrategia del negocio;

d) los lugares, dispositivos y recursos;

e) la legislación;

f) los contratistas, proveedores y clientes principales;

g) los procesos existentes, nuevos o retirados;

h) los riesgos (operativos o financieros).

15. CUMPLIMIENTO

15.1 Cumplimiento con los requisitos legales

OBJETIVO: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

El diseño, operación, uso y gestión de los sistemas de información puede estar sujeto a requisitos estatutarios, regulatorios y contractuales de seguridad.

Se debería buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales del derecho calificados. Los requisitos legales varían de un país a otro, al igual que en el caso de las transmisiones internacionales de datos (datos creados en un país y transmitidos a otro).

15.1.1 Identificación de la legislación aplicable

Control

Se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información.

Guía de Implementación

Los controles, medidas y responsabilidades específicos deben ser similarmente definidos y documentados para cumplir dichos requerimientos.

15.1.2 Derechos de propiedad intelectual (DPI)

Control

Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.

Guía de Implementación

Las siguientes pautas deben ser consideradas para proteger cualquier material que pueda ser considerado propiedad intelectual:

a) publicar una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información;

b) adquirir software solamente a través de fuentes conocidas para asegurar que el copyright no sea violado;

c) mantener la concientización sobre los derechos de autor del software y la política de adquisiciones, publicando la intención de adoptar medidas disciplinarias para el personal que los viole;

d) mantener los registros apropiados de activos e identificar todos los activos con requerimientos para proteger los derechos de la propiedad intelectual;

e) mantener los documentos que acrediten la propiedad de licencias, material original, manuales, etc.;

f) implantar controles para asegurar que no se exceda el número máximo de usuarios permitidos;

g) comprobar que sólo se instale software autorizado y productos bajo licencia;

h) establecer una política de mantenimiento de las condiciones adecuadas de la licencia;

i) establecer una política de eliminación de software o de su transferencia a terceros;

j) usar herramientas adecuadas de auditoria;

k) cumplir los términos y condiciones de uso del software y de la información obtenida de redes públicas;

l) no duplicar, convertir en otro formato o extraer de grabados comerciales (audio, filmaciones) lo que no sea permitido por la ley de copyright;

m) no copiar parcial o totalmente libros, artículos, reportes u otros documentos que no sean permitidos por la ley de copyright.

Otra Información

Los derechos de la propiedad intelectual incluyen al software o copyright del documento, derechos de diseño, marca registrada, patente y fuentes de licencia de código.

Los productos de software propietario son suministrados usualmente bajo un acuerdo de licencia que especifica los términos y condiciones, por ejemplo limitar el uso de productos para maquinas especificas o limitar el copiado solamente en la creación de las copias de respaldo. La situación de los derechos de la propiedad intelectual requiere ser esclarecido por el personal.

Los requisitos legislativos, regulatorios y contractuales pueden indicar restricciones en el copiado de material propietario. En particular, pueden requerir que solo se utilice el material que sea desarrollado por la organización o que sea licenciado o provisto por el creador a la organización. La infracción de copyright puede llevar a acciones legales que pueden involucrar procedimientos criminales.

15.1.3 Salvaguarda de los registros de la organización

Control

Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.

Guía de Implementación

Se debería clasificar los registros por tipos: registros contables, registros de bases de datos, registros de transacciones, registros de auditoria y procedimientos operativos, cada tipo con los detalles de sus plazos de retención y medios de almacenamiento (papel, microfichas, soporte magnético u óptico). Las claves criptográficas relacionadas con archivos cifrados o firmas digitales (véase el inciso 12.3) se deberían guardar de forma segura con el fin de habilitar el decriptado de los registros por el tamaño de tiempo que estos se encuentran retenidos.

Se debería considerar la posibilidad de degradación de los medios utilizados para almacenar los registros. Se deberían implantar procedimientos para su almacenamiento y utilización de acuerdo con las recomendaciones del fabricante. Para un almacenamiento a largo plazo, se puede considerar el uso de papel o de microfichas.
Cuando se utilicen medios electrónicos de almacenamiento se deberían incluir procedimientos que aseguren la capacidad de acceso a los datos (o sea, la legibilidad tanto del medio como

del formato) durante el plazo de retención, como objeto de salvaguardarlos contra su pérdida por futuros cambios de tecnología.

Se deberían elegir los sistemas de almacenamiento de datos para que éstos puedan recuperarse a tiempo y en un formato aceptable, dependiendo de los requisitos.

El sistema de almacenamiento y utilización debería asegurar una identificación clara de los registros y de su periodo de retención legal o regulatorio. Esto debería permitir la destrucción apropiada de los registros tras dicho periodo cuando ya no los necesite la organización.
Para dar cumplimiento a éstas obligaciones la organización debería dar los pasos siguientes:

a) se debería publicar guías sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;

b) se debería establecer un calendario de retenciones que identifique los períodos para cada tipo esencial de registros;

c) se debería mantener un inventario de las fuentes de información clave;

d) se deberían implantar los controles y medidas apropiadas para la protección de los registros y la información esencial contra su pérdida, destrucción o falsificación.

Otra Información

Es necesario guardar de forma segura ciertos registros, tanto para cumplir ciertos requisitos legales o regulatorios, como para soportar actividades esenciales del negocio. Por ejemplo, los registros que puedan requerirse para acreditar que la organización opera dentro de las reglas estatutarias o regulatorias, para asegurar una defensa adecuada contra una posible acción civil o penal, o bien para confirmar el estado financiero de la organización respecto a los accionistas, socios y auditores. La legislación nacional u otros reglamentos suelen establecer el plazo y contenido de la información a retener.

Para mayor información sobre el manejo de los registros organizacionales, se puede consultar la ISO 15489-1.

15.1.4 Protección de los datos y de la privacidad de la información personal

Control

La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales.

Guía de Implementación

Se debería implementar y desarrollar una política organizacional de privacidad y de protección de datos. Esta política debe ser comunicada a todo el personal implicado en el procesamiento de información personal.

El cumplimiento de la legislación de protección de datos personales requiere una estructura y controles de gestión apropiados. Este objetivo suele alcanzarse con mayor facilidad, designando un encargado de dicha protección que oriente a los directivos, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos a seguir. La responsabilidad para maniobrar información personal y asegurar el conocimiento de los principios de protección de datos debe ser confrontado con la legislación y regulaciones actuales. Se debería implementar medidas técnicas y organizacionales apropiadas para proteger la información personal.

Otra Información

Muchos países han establecido legislación colocando controles y medidas para el tratamiento y transmisión de datos personales (en general la información sobre personas físicas que pueda identificarlas). Dependiendo de la legislación nacional actual, estos controles y medidas suponen ciertas obligaciones a quien recoja, procese, ceda o comunique información personal, y puede restringir la posibilidad de transferir estos datos a otros países.

15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información

Control

El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.

Guía de Implementación

La organización debería proporcionar recursos informáticos para los fines del negocio. La gerencia debería autorizar su uso. Se debería considerar como impropio todo uso de estos recursos para fines no autorizados o ajenos al negocio (véase el inciso 6.1.4). Si dicha actividad se identifica mediante supervisión y control u otros medios, se debería poner en conocimiento del gerente responsable de adoptar la acción disciplinaria y/o legal apropiada.

Es esencial que todos los usuarios sean conscientes del alcance preciso del acceso que se les permite y del monitoreo que se lleva acabo para detecta un uso no autorizado. Esto puede conseguirse, por ejemplo, con una autorización escrita cuya copia debería firmar el usuario y ser almacenada por la organización. Se debería informar a los empleados de la organización y a usuarios de terceros que no se permitirá otro acceso que no sea el autorizado.

Al registrarse un usuario, un mensaje de advertencia debería indicar en la pantalla que el sistema al que se entra es privado y que no se permite el acceso no autorizado. El usuario tiene que darse por enterado y reaccionar de forma apropiada al mensaje para poder continuar el proceso de registro (véase el inciso 11.5.1).

Otra Información

Los recursos del tratamiento de la información de una organización son utilizados primaria y exclusivamente para propósitos de negocio.

La detección de un intruso, la inspección de contenido y otras herramientas de monitoreo ayudan a prevenir y detectar el mal uso de los recursos.

Muchos países tienen una legislación de protección contra el mal uso de la informática. El uso de un computador con fines no autorizados puede llegar a ser un delito penal.

La legalidad de la supervisión y el control del uso de los recursos, varía de un país a otro y puede requerir que se avise de su existencia a los empleados o que se requiera su consentimiento. Cuando el sistema al que se ingrese sea utilizado como acceso publico (por ejemplo un servidor de red) y este sujeto a monitoreo de seguridad, debería exhibirse un mensaje indicándolo.

15.1.6 Regulación de los controles criptográficos

Control

Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.

Guía de Implementación

Se debería considerar los siguientes ítems en conformidad con todos los acuerdos, leyes y regulaciones:

a) restricciones en la importación y/o exportación de hardware y software para realizar funciones criptográficas;

b) restricciones en la importación y/o exportación de hardware y software que incluya funciones criptográficas;

c) restricciones en el uso del encriptado;

d) métodos obligatorios o discrecionales de los países para acceder a la información que esté cifrada por hardware o software para proteger la confidencialidad de su contenido.

Se debería pedir asesoramiento legal para asegurar el cumplimiento de la legislación del país en la materia, así como antes de trasladar a otro país información cifrada o controles de cifrado.

15.2 Revisiones de la política de seguridad y de la conformidad técnica

OBJETIVO: Asegurar la conformidad de los sistemas con las políticas y normas de seguridad.

Se deberían hacer revisiones regulares de la seguridad de los sistemas de información.
Éstas se deberían atener a las políticas de seguridad apropiadas y se auditará el cumplimiento de las normas de implantación de la seguridad en los sistemas de información y en los controles de seguridad implementados.

15.2.1 Conformidad con la política de seguridad y los estándares

Control

Los gerentes deberían asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad.

Guía de Implementación

Los gerentes deben realizar revisiones regulares que aseguren el cumplimiento de las políticas y normas de seguridad.

Si se encuentra una no conformidad como resultado de la revisión, los gerentes deben de:

a) determinar las causas de la no conformidad;

b) evaluar la necesidad de acciones para asegurar que la no conformidad no vuelva a ocurrir;

c) determinar e implementar una acción correctiva apropiada;

d) revisar la acción correctiva que se realizo;

Los resultados de las revisiones y de las acciones correctivas llevadas a cabo por los gerentes deben ser grabados y mantenidos. Los gerentes deben reportar los resultados a las personas que llevan a cabo las revisiones independientes (véase el inciso 6.1.8), cuando dicha revisión es llevada a cabo en el área de su responsabilidad.

Otra Información

El seguimiento operativo del uso del sistema se cubre por el inciso 10.10.

15.2.2 Comprobación de la conformidad técnica

Control

Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información.

Guía de Implementación

La comprobación de la conformidad técnica debería ser realizada manualmente por un ingeniero de sistemas experimentado (con apoyo de herramientas lógicas apropiadas si es necesario), o bien automáticamente por un paquete que genere un informe técnico, a interpretar posteriormente por el especialista técnico.

Si se utilizan pruebas de intrusión o evaluaciones de vulnerabilidad, se debería tener cuidado debido a que estas actividades llegar a un compromiso de la seguridad del sistema. Estas pruebas deben ser planeadas, documentadas y repetibles.

Toda comprobación de la conformidad técnica sólo se debería realizar o supervisar por personas competentes y autorizadas.

Otra Información

La comprobación de la conformidad técnica implica examinar los sistemas operacionales con el fin de asegurar que los controles de hardware y software han sido implementados correctamente. Este tipo de comprobación de la conformidad requiere de un especialista técnico experto.

La comprobación de la conformidad también cubre, por ejemplo, pruebas de intrusión y evaluación de vulnerabilidades, que puede ser llevado a cabo por expertos independientes contratados específicamente para este propósito. Esto puede ser útil para la detección de vulnerabilidades en el sistema y para verificar que tan efectivos son los controles en prevenir el acceso no autorizado debido a estas vulnerabilidades.

Las pruebas de intrusión y las evaluaciones de vulnerabilidades proveen una foto del sistema en un estado específico y en un tiempo determinado. Esta foto esta limitada a esas partes del sistema que han sido probados durante los intentos de intrusión. Las pruebas de intrusión y evaluación de vulnerabilidades no son un substituto de la evaluación de riesgos.

15.3 Consideraciones sobre la auditoria de sistemas

OBJETIVO: Maximizar la efectividad y minimizar las interferencias en el proceso de auditoria del sistema.

Se deberían establecer controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoria.

15.3.1 Controles de auditoria de sistemas

Control

Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoria que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.

Guía de Implementación

Se debería observar las siguientes pautas:

a) deberían acordarse los requisitos de auditoria con la gerencia apropiada;

b) debería acordarse y controlarse el alcance de las verificaciones;

c) las verificaciones se deberían limitar a accesos solo de lectura al software y a los datos;

d) otro acceso distinto a solo lectura, únicamente se debería permitir para copias aisladas de archivos del sistema, que se deberían borrar cuando se termine la auditoria;

e) los recursos de tecnología de la información para realizar verificaciones deberían ser explícitamente identificados y puestos a disposición;

f) los requisitos para procesos especiales o adicionales deberían ser identificados y acordados;

g) todos los accesos deberían ser registrados y supervisados para producir un seguimiento de referencia; el uso de seguimiento de referencia de tiempo debe ser considerado para sistemas o datos críticos;

h) todos los procedimientos, requisitos y responsabilidades deberían estar documentados;

i) las personas que llevan a cabo la auditoria deben ser independientes de las actividades auditadas.

15.3.2 Protección de las herramientas de auditoria de sistemas

Control

Se deberían proteger los accesos a las herramientas de auditoria de sistemas con el fin de prever cualquier posible mal uso o daño.

Guía de Implementación

Las herramientas de auditoria de sistemas, por ejemplo, software o archivos de datos, deben estar separadas de los sistemas de desarrollo y de producción y no se mantendrán en librerías de cintas o en áreas de los usuarios, salvo que se les proporcione un nivel apropiado de protección adicional.

Otra Información

Si el personal experto esta implicado en la auditoria, puede existir un riesgo de mal uso de las herramientas de auditoria y de la información a la que acceden. Los controles como el 6.2.1 (para determinar los riesgos) y 9.1.2 (para restringir el acceso físico) pueden ser considerados para tratar estos riesgos y se debe tomar consecuencia como el cambio inmediato de contraseñas divulgadas a los auditores.

16. ANTECEDENTES

16.1.	ISO/IEC 17799:2000	Information technology – Code of practice for information security management
16.2.	UNE-ISO/IEC 17799:2002	Tecnología de la información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.