Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. TECNOLOGIA DE LA INFORMACIÓN. CODIGO DE BUENAS PRACTICAS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION. 1ª EDICIÓN" en entidades del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL
N° 224-2004-PCM

Lima, 23 de julio de 2004

CONSIDERANDO:

Que, de conformidad con el artículo 2º del Decreto Supremo Nº 066-2003-PCM y el numeral 3.10 del artículo 3º y artículo 22º del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 067-2003-PCM, la Presidencia del Consejo de Ministros se encarga de normar, coordinar, integrar y promover el desarrollo de la actividad informática en la Administración Pública, impulsando y fomentando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del Estado, actúa como ente rector del Sistema Nacional de Informática, y dirige y supervisa la política nacional de informática y gobierno electrónico;

Que, mediante Resolución de la Comisión de Reglamentos Técnicos y Comerciales N° 0026-2004/CRT-INDECOPI se aprobó como Norma Técnica Peruana la ***"****NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1ª Edición****"***;

Que, la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, en coordinación con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, ha recomendado la aplicación y uso obligatorio de la Norma Técnica Peruana antes mencionada en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar a la creación de la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente importante para dicho objetivo;

De conformidad con lo dispuesto por el Decreto Legislativo Nº 560 - Ley del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo Nº 067-2003-PCM,

SE RESUELVE:

Artículo 1º.- Aprobar el uso obligatorio de la Norma Técnica Peruana ***"****NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1ª Edición****"***, en todas las Entidades integrantes del Sistema Nacional de Informática, documento que será publicado en el portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe).

Artículo 2º.- La Norma Técnica Peruana señalada en el artículo precedente, se aplicará a partir del día siguiente de la publicación de la presente Resolución Ministerial, teniendo las Entidades antes mencionadas un plazo de dieciocho (18) meses para su implantación, por lo que deberán considerar en sus respectivos Planes Operativos Informáticos (POI) las actividades necesarias con esa finalidad.

Regístrese, comuníquese y publíquese.

CARLOS FERRERO
Presidente del Consejo de Ministros

Oficina Nacional de Gobierno Electrónico e Informática

Presidencia del Consejo de Ministros

TECNOLOGÍA DE LA INFORMACIÓN. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

HOJA DE INFORMACION GENERAL

CONTROL DOCUMENTAL:

PROCEDIMIENTO:	NTP - ISO/IEC 17799:2004
PROYECTO:	Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
ENTIDAD:	Presidencia del Consejo de Ministros
VERSIÓN:	1.0
FECHA EDICIÓN:	07/07/2004
NOMBRE DE ARCHIVO:	P01-PCM-ISO17799-001v1.doc
RESUMEN:	La presente Norma Técnica Peruana establece recomendaciones para realizar la gestión de la seguridad de la información, que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Tiene por objeto proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones de la Administración Pública y ser una práctica eficaz de la gestión de la seguridad, así como proporcionar confianza en las relaciones de intercambio de información entre organizaciones públicas. Las recomendaciones que se establecen en esta NTP deberían elegirse y utilizarse de acuerdo con la legislación aplicable en la materia. (Aprobada con R. 0026-2004/CRT-INDECOPI).

CONTROL DE VERSIONES

FUENTE DE CAMBIO	FECHA DE SOLICITUD DEL CAMBIO	VERSIÓN	PARTES QUE CAMBIAN	DESCRIPCIÓN DEL CAMBIO	FECHA DE CAMBIO
P01-PCM-ISO17799-001v1doc		1.00	N/A		

TECNOLOGÍA DE LA INFORMACIÓN. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1ª Edición

NTP - ISO/IEC 17799:2004

INDICE

		Página
	PREFACIO	ix
	INTRODUCCIÓN	
	¿Qué es la seguridad de la información?	1
	¿Por qué es necesaria la seguridad de la información?	1
	¿Cómo establecer los requisitos de seguridad?	2
	Evaluación de los riesgos contra la seguridad	2
	Selección de controles	3
	Punto de partida de la seguridad de la información	4
	Factores críticos de éxito	5
	Desarrollo de directrices propias	6
1.	**OBJETO Y CAMPO DE APLICACIÓN**	7
2.	**TERMINOS Y DEFINICIONES**	
2.1	Seguridad de la información	7
2.2	Evaluación del riesgo	7
2.3	Gestión del riesgo	8
3	**POLITICA DE SEGURIDAD**	
3.1	Política de seguridad de la información	8
3.1.1	Documento de política de seguridad de la información	8
3.1.2	Revisión y evaluación	9
4.	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**	
4.1	Estructura para la seguridad de la información	10
4.1.1	Comité de gestión de seguridad de la información	10
4.1.2	Coordinación de la seguridad de la información	11
4.1.3	Asignación de responsabilidades para la seguridad de la información	11
4.1.4	Proceso de autorización de recursos para el tratamiento de la información	12
4.1.5	Asesoramiento de especialista en seguridad de la información	13
4.1.6	Cooperación entre organizaciones	13
4.1.7	Revisión independiente de la seguridad de la información	14
4.2	Seguridad en los accesos de terceras partes	14
4.2.1	Identificación de riesgos por el acceso de terceros	15
4.2.2	Requisitos de seguridad en contratos con terceros	16
4.3	Outsourcing	18
4.3.1	Requisitos de seguridad en contratos de outsourcing	18

		Página
5.	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	
5.1	Responsabilidad sobre los activos	19
5.1.1	Inventario de archivos	19
5.2	Clasificación de la información	20
5.2.1	Guías de clasificación	20
5.2.2	Marcado y tratamiento de la información	21
6.	**SEGURIDAD LIGADA AL PERSONAL**	
6.1	Seguridad en la definición del trabajo y los recursos	22
6.1.1	Inclusión de la seguridad en las responsabilidades laborales	22
6.1.2	Selección y política de personal	22
6.1.3	Acuerdos de confidencialidad	23
6.1.4	Términos y condiciones de la relación laboral	23
6.2	Formación de usuarios	24
6.2.1	Formación y capacitación en seguridad de la información	24
6.3	Respuesta ante incidencias y malos funcionamientos de la seguridad	24
6.3.1	Comunicación de las incidencias de seguridad	25
6.3.2	Comunicación de las debilidades de seguridad	25
6.3.3	Comunicación de los fallos del software	25
6.3.4	Aprendiendo de las incidencias	26
6.3.5	Procedimiento disciplinario	26
7.	**SEGURIDAD FÍSICA Y DEL ENTORNO**	
7.1	Áreas seguras	26
7.1.1	Perímetro de seguridad física	27
7.1.2	Controles físicos de entrada	27
7.1.3	Seguridad de oficinas, despachos y recursos	28
7.1.4	El trabajo en las áreas seguras	29
7.1.5	Áreas aisladas de carga y descarga	29
7.2	Seguridad de los equipos	30
7.2.1	Instalación y protección de equipos	30
7.2.2	Suministro eléctrico	31
7.2.3	Seguridad del cableado	32
7.2.4	Mantenimiento de equipos	33
7.2.5	Seguridad de equipos fuera de los locales de la organización	33
7.2.6	Seguridad en el reuso o eliminación de equipos	34
7.3.	Controles generales	34
7.3.1	Política de puesto de trabajo despejado y bloqueo de pantalla	35
7.3.2	Extracción de pertenencias	35
8.	**GESTION DE COMUNICACIONES Y OPERACIONES**	
8.1	Procedimientos y responsabilidades de operación	36
8.1.1	Documentación de procedimientos operativos	36

Página

8.1.2	Control de cambios operacionales	37
8.1.3	Procedimientos de gestión de incidencias	37
8.1.4	Segregación de tareas	39
8.1.5	Separación de los recursos para desarrollo y para producción	39
8.1.6	Gestión de servicios externos	40
8.2	Planificación y aceptación del sistema	41
8.2.1	Planificación de la capacidad	41
8.2.2	Aceptación del sistema	41
8.3	Protección contra software malicioso	42
8.3.1	Medidas y controles contra software malicioso	43
8.4	Gestión interna de respaldo y recuperación	44
8.4.1	Recuperación de la información	44
8.4.2	Diarios de operación	45
8.4.3	Registro de fallos	45
8.5	Gestión de redes	45
8.5.1	Controles de red	46
8.6	Utilización y seguridad de los medios de información	46
8.6.1	Gestión de medios removibles	46
8.6.2	Eliminación de medios	47
8.6.3	Procedimientos de manipulación de la información	48
8.6.4	Seguridad de la documentación de sistemas	49
8.7	Intercambio de información y software	49
8.7.1	Acuerdos para intercambio de información y software	49
8.7.2	Seguridad de medios en tránsito	50
8.7.3	Seguridad en comercio electrónico	51
8.7.4	Seguridad del correo electrónico	52
8.7.5	Seguridad de los sistemas ofimáticos	53
8.7.6	Sistemas públicamente disponibles	54
8.7.7	Otras formas de intercambio de información	55
9.	**CONTROL DE ACCESOS**	
9.1	Requisitos de negocio para el control de accesos	56
9.1.1	Política de control de accesos	56
9.2	Gestión de acceso de usuarios	57
9.2.1	Registro de usuario	58
9.2.2	Gestión de privilegios	59
9.2.3	Gestión de contraseñas de usuario	59
9.2.4	Revisión de los derechos de acceso de los usuarios	60
9.3	Responsabilidades de los usuarios	60
9.3.1	Uso de contraseña	60
9.3.2	Equipo informático de usuario desatendido	62
9.4	Control de acceso a la red	62

9.4.1	Política de uso de los servicios de la red	62
9.4.2	Ruta forzosa	63
9.4.3	Autenticación de usuarios para conexiones externas	64
9.4.4	Autenticación de nodos de la red	64
9.4.5	Protección a puertos de diagnóstico remoto	65
9.4.6	Segregación en las redes	65
9.4.7	Control de conexión a las redes	66
9.4.8	Control de enrutamiento en la red	66
9.4.9	Seguridad de los servicios de red	66
9.5	Control de acceso al sistema operativo	67
9.5.1	Identificación automática de terminales	67
9.5.2	Procedimientos de conexión de terminales	67
9.5.3	Identificación y autenticación del usuario	68
9.5.4	Sistema de gestión de contraseñas	69
9.5.5	Utilización de las facilidades del sistema	70
9.5.6	Protección del usuario frente a coacciones	70
9.5.7	Desconexión automática de terminales	70
9.5.8	Limitación del tiempo de conexión	71
9.6	Control de acceso a las aplicaciones	71
9.6.1	Restricción de acceso a la información	72
9.6.2	Aislamiento de sistemas sensibles	72
9.7	Seguimiento de accesos y usos del sistema	73
9.7.1	Registro de incidencias	73
9.7.2	Seguimiento del uso de los sistemas	73
9.7.3	Sincronización de relojes	75
9.8	Informática móvil y teletrabajo	76
9.8.1	Informática móvil	76
9.8.2	Teletrabajo	77
10.	**DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
10.1	Requisitos de seguridad de los sistemas	78
10.1.1	Análisis y especificación de los requisitos de seguridad	78
10.2	Seguridad de las aplicaciones del sistema	79
10.2.1	Validación de los datos de entrada	79
10.2.2	Control del proceso interno	80
10.2.3	Autenticación de mensajes	81
10.2.4	Validación de los datos de salida	81
10.3	Controles criptográficos	82
10.3.1	Política de uso de los controles criptográficos	82
10.3.2	Cifrado	83
10.3.3	Firmas digitales	83
10.3.4	Servicios de no repudio	84
10.3.5	Gestión de claves	84

Página

10.4	Seguridad de los archivos del sistema	86
10.4.1	Control del software en producción	87
10.4.2	Protección de los datos de prueba del sistema	87
10.4.3	Control de acceso a la librería de programas fuente	88
10.5	Seguridad en los procesos de desarrollo y soporte	89
10.5.1	Procedimientos de control de cambios	89
10.5.2	Revisión técnica de los cambios en el sistema operativo	90
10.5.3	Restricciones en los cambios a los paquetes de software	90
10.5.4	Canales encubiertos y código Troyano	91
10.5.5	Desarrollo externo del software	91
11	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**	
11.1	Aspectos de la gestión de continuidad del negocio	92
11.1.1	Proceso de gestión de la continuidad del negocio	92
11.1.2	Continuidad del negocio y análisis de impactos	93
11.1.3	Redacción e implantación de planes de continuidad	93
11.1.4	Marco de planificación para la continuidad del negocio	94
11.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad	95
12.	**CUMPLIMIENTO**	
12.1	Cumplimiento con los requisitos legales	97
12.1.1	Identificación de la legislación aplicable	97
12.1.2	Derechos de propiedad intelectual (DPI)	97
12.1.3	Salvaguarda de los registros de la organización	98
12.1.4	Protección de los datos y de la privacidad de la información personal	99
12.1.5	Evitar el mal uso de los recursos de tratamiento de la información	100
12.1.6	Regulación de los controles criptográficos	100
12.1.7	Recopilación de pruebas	101
12.2	Revisiones de la política de seguridad y de la conformidad técnica	102
12.2.1	Conformidad con la política de seguridad	102
12.2.2	Comprobación de la conformidad técnica	103
12.3	Consideraciones sobre la auditoria de sistemas	103
12.3.1	Controles de auditoría de sistemas	103
12.3.2	Protección de las herramientas de auditoría de sistemas	104
13	**ANTECEDENTES**	105

PREFACIO

A. RESEÑA HISTORICA

A.1. La Presente Norma Técnica Peruana fue elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos (EDI), mediante el Sistema 2 u Ordinario, durante los meses de agosto y setiembre del 2,003.

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 2003-12-04, el **PNTP ISO/IEC 17799:2003. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información**, para su revisión y aprobación, previa a la etapa de discusión pública.

A.3. La presente Norma Técnica Peruana utilizó como antecedentes la norma ISO/IEC 17799: 2000. Information Technology – Code of practice for information security management y la norma UNE-ISO/IEC 17799: 2002. Tecnología de la información. Código de buenas prácticas para la Gestión de la Seguridad. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurado de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

A.4. La presente Norma Técnica fue aprobada por resolución N° 0026-2004/CRT-INDECOPI.

A.5. La presente Norma Técnica es ahora asumida por el Sistema Nacional de Informática. (Toda mención al término “negocio” en esta adopción, está referida al fin o propósito de las actividades de la Institución Pública o a la misma Institución Pública, según el contexto).

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACION DEL PROYECTO DE NORMA TECNICA PERUANA

Secretaría	**EAN PERU**
Presidente	Marco Suárez
Secretaria	Mary Wong

ENTIDAD	REPRESENTANTE
DISTRIBUIDORA MAYORISTA SYMBOL S.A.	Adela Barcenas
E. WONG S.A.	Rubén Dueñas Iris Cabrera
GESTIONA S.A.	Joaquín Valera
IBC SOLUTIONS PERU S.A.C.	Oscar Velásquez Daniela Orellana
IND. PACOCHA S.A.	Juan Luis Villavicencio Hernaldo Alva
OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA – PCM	Max Lazaro Cesar Vilchez
LIMATEL	Pablo Omonte
PONT. UNIV. CATOLICA DEL PERU	Viktor Khlebnikov Willy Carrera
PROCTER & GAMBLE PERU S.R.L.	Jesús Ríos
TRANSPORTE CONFIDENCIAL DE INFORMACION S.A.	Renzo Alcántara Jenny Hermosilla
EAN PERU	Milagros Dávila Tatiana Peña

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. 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 negocio.

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 se caracteriza aquí como la preservación de:

a) su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;

b) su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;

c) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

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. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

¿Por qué es necesaria la seguridad de información?

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, 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 dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. 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 unos 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.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

¿Cómo establecer los requisitos de seguridad?

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

La primera fuente procede de la valoración de los riesgos de la organización. 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.

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.

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. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, sólo a partes de ella o incluso a sistemas de información individuales, a componentes específicos de sistemas o a servicios dónde sea factible, realista y útil.

La evaluación del riesgo es una consideración sistemática:

a) del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

b) de la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

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. El proceso de evaluación de riesgos y selección de controles, puede requerir que sea realizado varias veces para cubrir partes diferentes de la organización o sistemas de información individuales.

Es importante, efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

a) tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización;

b) considerar nuevas amenazas y vulnerabilidades;

c) confirmar que las medidas de control siguen siendo eficaces y apropiadas.

Deberían realizarse estas revisiones con distintos niveles de detalle dependiendo de los resultados de las evaluaciones previas y de los umbrales de riesgo que la gerencia está dispuesta a aceptar. Se suelen realizar las evaluaciones de riesgo primero a alto nivel, como un medio de priorizar recursos en áreas de alto riesgo, y después en un nivel más detallado para enfocar riesgos específicos.

Selección de controles

Una vez que los requisitos de seguridad han sido identificados, 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. Hay muchas formas distintas de gestionar los riesgos y este documento proporciona ejemplos de enfoques habituales. Sin embargo hay que reconocer que ciertos controles no son aplicables para todos los sistemas o entornos de información y pueden no ser de aplicación en todas las organizaciones. Por ejemplo, en el inciso 8.1.4 se describe como pueden segregarse ciertas tareas para evitar fraudes y errores. Las organizaciones pequeñas podrían no segregar todas las tareas y necesitarían otras formas para conseguir

el mismo objetivo de control. Por poner otro ejemplo, los incisos 9.7 y 12.1 describen como puede hacerse el seguimiento del uso del sistema y recogerse evidencias. Las medidas de control descritas como el registro de eventos podrían entrar en conflicto con la legislación aplicable, como la referente a la protección de la intimidad de los datos de carácter personal de los clientes o de los datos laborales.

Los controles deberían elegirse por su costo de implantación en relación con los riesgos a reducir y con las posibles pérdidas si se materializa la ruptura de seguridad. También es conveniente tener en cuenta factores no económicos como la pérdida de reputación.

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".

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 12.1.4);

b) la salvaguarda de los registros de la organización (véase el inciso 12.1.3);

c) los derechos de la propiedad intelectual (véase el inciso 12.1.2).

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 3.1);

b) la asignación de responsabilidades de seguridad (véase el inciso 4.1.3);

c) la formación y capacitación para la seguridad de la información (véase el inciso 6.2.1);

d) el registro de las incidencias de seguridad (véase el inciso 6.3.1);

e) la gestión de la continuidad del negocio (véase el inciso 11.1).

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 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) la formación y capacitación adecuadas;

h) 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.

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 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, así como 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 Seguridad de la Información

Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Confidencialidad**
  Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

- **Integridad**
  Garantía de la exactitud y el contenido completo de la información y los métodos de su procesamiento.

- **Disponibilidad**
  Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados,

2.2 Evaluación del Riesgo

Proceso de evaluación de las amenazas, impactos y vulnerabilidades de la información y de los medios de tratamiento de la información y de su probable ocurrencia.

2.3 Gestión del Riesgo

Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a los sistemas de información.

3. POLÍTICA DE SEGURIDAD

3.1 Política de seguridad de la información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información.

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.

3.1.1 Documento de política de seguridad de la información

La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. 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 la 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) 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) prevención y detección de virus y otro software malicioso;

4) gestión de la continuidad del negocio;

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

d) 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;

e) 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.

3.1.2 Revisión y evaluación

La política debería tener un propietario que sea responsable de su mantenimiento y revisión conforme a un proceso de revisión definido. Este proceso debería asegurar que la revisión responde a todo cambio que afecte a las bases de la evaluación original de riesgo, por ejemplo, incidencias de seguridad significativas, nuevas vulnerabilidades o cambios a la infraestructura organizacional o técnica. También deberían programarse revisiones periódicas de:

a) la efectividad de la política, demostrada por la naturaleza, número e impacto de las incidencias de seguridad registradas;

b) el costo y el impacto de los controles en la eficiencia del negocio;

c) los efectos de los cambios a la tecnología.

4. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

4.1 Estructura para la seguridad de la información

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 especializada 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, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.

4.1.1 Comité de gestión de seguridad de la información

La seguridad de la información es una responsabilidad organizativa que debería ser compartida por todos los miembros de la gerencia. Sin embargo debería establecerse un comité que asegure una dirección clara y el apoyo visible de la gerencia a las iniciativas de seguridad. Este comité debería promover la seguridad en la organización por medio de un compromiso apropiado y de los recursos adecuados. El comité debería formar parte de la estructura directiva existente. Normalmente este comité realiza las siguientes funciones:

a) revisión y aprobación de la política de seguridad de la información y de las responsabilidades principales;

b) supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales;

c) revisión y seguimiento de las incidencias en la seguridad de la información;

d) aprobación de las iniciativas principales para mejorar la seguridad de la información.

Un miembro de la gerencia debería responsabilizarse de todas las actividades relacionadas con la seguridad.

4.1.2 Coordinación de la seguridad de la información

En una organización grande puede ser necesario coordinar la implantación de los controles de seguridad de la información por medio de un comité interfuncional de directivos que representen a las áreas más importantes de la organización. Normalmente este comité:

a) establece las funciones y responsabilidades específicas de seguridad de la información en toda la organización;

b) acuerda métodos y procesos específicos para la seguridad de la información, por ejemplo, análisis de riesgos, el sistema de clasificación de la información;

c) establece y respalda las iniciativas de seguridad de la información en toda la organización, por ejemplo, el programa de capacitación en seguridad;

d) asegura que la seguridad forma parte del proceso de planificación de la información;

e) evalúa la adecuación y coordina la implantación de los controles de seguridad de la información específicos para nuevos sistemas o servicios;

f) revisa las incidencias sobre seguridad de la información;

g) da conocimiento del apoyo gerencial a la seguridad de la información en toda la organización.

4.1.3 Asignación de responsabilidades sobre seguridad de la información

Deberían definirse claramente las responsabilidades para la protección de los activos individuales y para la ejecución de los procesos específicos de seguridad.

La política de seguridad de la información (véase el capítulo 3) debería servir de guía para la asignación de las funciones y responsabilidades de seguridad en la organización. 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.

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.

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.

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

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

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.

NOTA: Ciertas conexiones requieren la aprobación de su tipo.

c) Debería autorizarse el uso de medios informáticos personales para el tratamiento de la información de la organización así como los controles necesarios.

d) El uso en el puesto de trabajo de medios informáticos personales puede causar nuevas vulnerabilidades, que deberían evaluarse y autorizarse.

Estos controles son especialmente importantes en un entorno de red.

4.1.5 Asesoramiento de especialistas en seguridad de la información

Numerosas organizaciones pueden necesitar el asesoramiento de especialistas en seguridad. Idealmente, un asesor interno experto en seguridad de la información debería proporcionar este soporte. No todas las organizaciones desean tener como empleado un asesor especializado. En este caso se recomienda identificar una persona específica que coordine el conocimiento y las experiencias internas para asegurar la consistencia de las decisiones de seguridad y ayudar en su desarrollo. En cualquier caso deberían tener también acceso a asesores externos adecuados que aporten la ayuda especializada que supere la propia experiencia interna.

Se debería encargar a los asesores en seguridad de la información o las personas de contacto equivalente, que asesoren en todos los aspectos de la seguridad de la información, utilizando asesoramiento ya sea propio o externo. La calidad de sus evaluaciones en cuanto a amenazas de seguridad y de su asesoría sobre los controles determinará la efectividad de la seguridad de la información en la organización. Para obtener una eficacia e influencia máximas, estos especialistas deberían tener acceso directo a los órganos de gerencia de la organización.

El especialista en seguridad de la información, o la persona de contacto equivalente, debería ser consultado lo más rápidamente posible cuando se produzca una incidencia sospechosa o un fallo de seguridad, para proporcionar fuentes expertas o recursos de investigación del problema. Aunque la mayoría de las investigaciones internas se desarrollen bajo el control de la gerencia, el asesor de seguridad de la información puede consultarse para aconsejar, dirigir o conducir la investigación.

4.1.6 Cooperación entre organizaciones

Deberían mantenerse contactos con las autoridades encargadas de hacer cumplir la legislación, los organismos reguladores, los proveedores de servicios de información y los operadores de telecomunicaciones para asegurar que se obtiene su asesoramiento y se adopta rápidamente la acción adecuada en caso de incidencia de seguridad. Igualmente debería considerarse el interés de pertenecer a grupos de seguridad y foros industriales.

Deberían restringirse los intercambios de información sobre seguridad para impedir que personas no autorizadas puedan acceder a información confidencial de la organización.

4.1.7 Revisión independiente de la seguridad de la información.

El documento de política de seguridad de la información (véase el inciso 3.1) establece la política y las responsabilidades sobre seguridad de la información. Su implantación debería revisarse de forma independiente para asegurar que las practicas de la organización reflejan dicha política y que además ésta es realizable y eficaz (véase el inciso 12.2).

Dichas revisiones pueden realizarse por la función interna de auditoria, por un gestor independiente o por otra organización especializada en tales revisiones, siempre que estos candidatos tengan la experiencia y conocimientos apropiados.

4.2 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.

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.

El acceso de un tercero puede implicar a otros participantes. Los contratos que confieren acceso a un tercero deberían incluir la posibilidad de designar a otros participantes y las condiciones para su acceso.

Esta norma podría usarse como base para dichos contratos y cuando se considere el outsourcing del tratamiento de la información.

4.2.1 Identificación de riesgos por parte de terceros

4.2.1.1 Tipos de acceso

El tipo de acceso que se da a un tercero tiene especial importancia. Así los riesgos de acceso de su conexión a una red son distintos a los de un acceso físico. Se deberían considerar estos tipos de acceso:

a) acceso físico, por ejemplo, a despachos, centros de cálculo, bibliotecas de archivos;

b) acceso lógico, por ejemplo, a bases de datos o a sistemas de información de la organización.

4.2.1.2 Motivos de acceso

En algunos casos, terceros han de tener acceso garantizado por diversos motivos. Hay terceros que han de tener acceso físico y lógico porque dan servicio a la organización, sin estar instalados en ella, por ejemplo:

a) el personal de soporte al hardware y al software requieren acceso en el nivel del sistema o de las funcionalidades de bajo nivel de las aplicaciones;

b) asociados o partícipes en el negocio que han de intercambiar información, acceder a los sistemas de información o compartir bases de datos.

La información puede estar expuesta a cierto riesgo, debido al acceso por terceros, sin una administración adecuada de la seguridad. Cuando por necesidades de la organización se necesite conectar a un tercero, debería realizarse una evaluación de riesgos para identificar los requisitos para los controles específicos. Debería tenerse en cuenta el tipo de acceso requerido, el valor de la información, las medidas de control empleadas por el tercero y las implicaciones que dicho acceso representa para la seguridad de la información de la organización.

4.2.1.3 Subcontratados trabajando en la organización

Los terceros que trabajan en la organización de forma temporal también pueden aumentar las debilidades de la seguridad. Ejemplos de dichos terceros serían:

a) el personal de mantenimiento y soporte de hardware y software;

b) los servicios de soporte externalizados de limpieza, cafetería, vigilancia y otros;

c) los estudiantes en prácticas u otros contratados por tiempo limitado;

d) los consultores.

Es esencial comprender qué medidas de control se necesitan para administrar el acceso de estos terceros a los recursos de tratamiento de información. En general, los contratos de terceros deberían reflejar todos los requisitos sobre seguridad y los controles internos que requiera el acceso de aquellos (véase también el inciso 4.2.2). Si, por ejemplo, hay una especial necesidad de confidencialidad en la información, deberían establecerse cláusulas de no divulgación (véase el inciso 6.1.3).

No se debería dar acceso a terceros a los recursos de información y de su tratamiento hasta que no se hayan implantado las medidas de control apropiadas y firmado el contrato que establezca los términos de conexión o acceso.

4.2.2 Requisitos de seguridad en contratos con terceros

Los acuerdos que permiten el acceso de terceros a recursos de tratamiento de información de la organización deberían estar basados en un contrato formal que contenga o se refiera a todos los requisitos de seguridad que cumplan las políticas y normas de seguridad de la organización. El contrato debería asegurar que no hay malentendidos entre la organización y los terceros. Las organizaciones deberían verse compensadas hasta la indemnización de sus suministradores. Los siguientes términos deberían considerarse para su inclusión en el contrato:

a) la política general sobre seguridad de la información;

b) una protección de activos que incluya:

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) controles para asegurar la recuperación o destrucción de la información y los activos al terminar el contrato o en algún momento acordado dentro del periodo de vigencia del contrato;

4) medidas de integridad y disponibilidad;

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

c) la descripción de cada servicio disponible;

d) los niveles de servicio deseados y los niveles inaceptables;

e) previsiones para traslados de personal cuando sea oportuno;

f) las respectivas obligaciones de las partes en los acuerdos;

g) 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 12.1);

h) los derechos de propiedad intelectual, protección contra copias (véase el inciso 12.1.2.) y protección en tareas de colaboración (véase también el inciso 6.1.3);

i) 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) los requisitos para mantener actualizada la lista de usuarios autorizados al acceso de servicios ofrecidos con los correspondientes derechos y privilegios;

j) la definición, seguimiento y comunicación de criterios verificables de rendimiento;

k) el derecho para controlar, y suspender en su caso, la actividad de los usuarios;

l) el derecho de auditar directamente o por terceros el cumplimiento de las responsabilidades contractuales;

m) el establecimiento de un procedimiento de escalado para la resolución de los problemas, siendo conveniente la consideración cuando sea preciso, de acuerdos en caso de contingencia;

n) responsabilidades sobre la instalación y mantenimiento del hardware y del software;

o) una estructura clara sobre los formatos y comunicación de los informes;

p) un procedimiento claro y bien especificado de gestión del cambio;

q) los controles necesarios de protección física y los mecanismos que aseguren su cumplimiento;

r) la formación del administrador y los usuarios en los métodos y procedimientos de seguridad;

s) controles para asegurar la protección contra software malicioso (véase el inciso 8.3);

t) acuerdos para informar, notificar e investigar las incidencias y fallos de seguridad;

u) la implicación de los terceros con sus subcontratistas.

4.3 Outsourcing

OBJETIVO: Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización. Los acuerdos de outsourcing deberían incluir en el contrato entre las partes, los riesgos, controles y procedimientos de seguridad para sistemas de información, entornos de redes y terminales.

4.3.1 Requisitos de seguridad en contratos de outsourcing

Los requisitos de seguridad de una organización que externaliza la gestión y el control de parte o de todos sus sistemas de información, entornos de redes y terminales deberían incluirse en el contrato entre las partes.

Por ejemplo el contrato debería incluir:

a) cómo cumplir los requisitos legales (por ejemplo los de protección de datos);

b) qué acuerdos establecer para asegurar que las partes implicadas en el outsourcing, incluidos los subcontratistas, conocen sus responsabilidades en materia de seguridad;

c) cómo deberían mantenerse y probarse la integridad y la confidencialidad de los activos de la organización;

d) qué controles físicos y lógicos deberían usarse para limitar o restringir a los usuarios autorizados el acceso a la información sensible de la organización;

e) cómo mantener la disponibilidad de los servicios en caso de desastre;

f) qué niveles de seguridad física deberían proporcionarse al equipo outsourcing;

g) el derecho de auditar.

Deberían considerarse como parte del contrato los términos de la lista del inciso 4.2.2. El contrato debería permitir la ampliación de los requisitos y procedimientos de seguridad en un plan de gestión de seguridad a acordar entre las partes.
Los contratos de outsourcing pueden contener cuestiones complejas sobre seguridad, pero los controles incluidos en este código pueden servir como punto de partida para acordar la estructura y el contenido del plan de gestión de seguridad.

5. CLASIFICACIÓN Y CONTROL DE ACTIVOS

5.1 Responsabilidad sobre los activos

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

Se debería adjudicar la responsabilidad de todos los activos de información importantes y se debería asignar un propietario. La responsabilidad sobre los activos ayuda a asegurar que se mantiene la protección adecuada. 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

5.1.1 Inventario de activos

Los inventarios de los activos ayudan a asegurar que se inicia 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. Sobre la base de esta información la organización puede proporcionar niveles de protección proporcionales a dicho valor e importancia. Debería establecerse y mantenerse el inventario de los activos importantes asociados con cada sistema de información. Cada activo debería identificarse claramente, y acordarse y documentarse la clasificación de su seguridad y pertenencia (véase el inciso 5.2), junto a su situación habitual (crucial cuando se tenga que recuperarlo de una pérdida o daño). Por ejemplo, éstos son activos asociados con los sistemas de información:

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 tratamiento (procesadores, monitores, portátiles, módems), equipo de comunicaciones (routers, centrales digitales, máquinas de fax), medios magnéticos (discos y cintas), otro equipo técnico (suministro de energía, unidades de aire acondicionado), muebles, etc.

d) servicios: servicios de tratamiento y comunicaciones, servicios generales (calefacción, alumbrado, energía, aire acondicionado).

5.2 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.

5.2.1 Guías de clasificación

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, por ejemplo, el acceso no autorizado o el daño a la información. En general la clasificación que se da a la información es una forma abreviada de determinar cómo manejarla y protegerla.

La información y los resultados de los sistemas que manejan datos clasificados deberían catalogarse en relación con su valor e importancia para la organización. También puede ser adecuado catalogar la información en términos de su criticidad - por ejemplo de su integridad y disponibilidad - para la organización.

La información suele dejar de tener importancia o criticidad tras cierto tiempo, por ejemplo, cuando se ha hecho pública. Estos aspectos deberían considerarse, puesto que una sobre-clasificación conllevaría un gasto adicional innecesario. Las guías de clasificación deberían prever que la clasificación de cualquier elemento de información no tiene por que estar definida para siempre y que puede cambiar de acuerdo con ciertas políticas predeterminadas (véase el inciso 9.1).

Debería considerarse el número de categorías de clasificación y los beneficios obtenidos con su uso. Los esquemas demasiado complejos pueden ser impracticables por molestos o costosos. Es conveniente cuidar la interpretación de los catálogos de clasificación de otras organizaciones que pueden tener distintas definiciones de conceptos iguales o llamados de forma similar.

El responsable de definir y revisar periódicamente la clasificación de un elemento de información, por ejemplo, un documento, registro, archivo o disco debería seguir siendo del creador o el propietario nombrado de la información.

5.2.2 Marcado y tratamiento de la información

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. Dichos procedimientos han de cubrir los activos en formato físico y electrónico. Para cada clasificación los procedimientos de utilización deberían cubrir los siguientes tipos de actividad de tratamiento de información:

a) copia;

b) almacenamiento;

c) transmisión por correo, fax y correo electrónico;

d) transmisión oral, incluida telefonía móvil, transmisión de voz y máquinas de respuesta automática;

e) destrucción.

La salida procedente de los sistemas que traten información clasificada como sensible o crítica debería llevar una etiqueta de clasificación adecuada (en la salida). El marcado debería reflejar la clasificación de acuerdo con las reglas establecidas en el inciso 5.2.1. Se consideran elementos como informes impresos, pantallas, medios de almacenamiento (cintas, discos, CDs, casetes), mensajes electrónicos y transferencias de archivos.

Las etiquetas físicas suelen ser la forma más apropiada de marcado. Sin embargo, ciertos activos de información, como los documentos en formato electrónico no pueden marcarse físicamente y hay que usar medios electrónicos de marcado.

6. SEGURIDAD LIGADA AL PERSONAL

6.1 Seguridad en la definición del trabajo y los recursos

OBJETIVO: Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.

La seguridad debería contemplarse desde las etapas de selección de personal, incluirse en los contratos y seguirse durante el desarrollo de la relación laboral.

Deberían filtrarse adecuadamente los candidatos (véase el inciso 6.1.2), sobre todo para tareas sensibles. Todos los empleados y los terceros, usuarios de aplicaciones de tratamiento de información, deberían firmar una cláusula de confidencialidad (no divulgación).

6.1.1 Inclusión de la seguridad en las responsabilidades laborales

Las funciones y responsabilidades sobre la seguridad de la información, de acuerdo con la política de seguridad de la organización (véase el inciso 3.1), deberían documentarse cuando sea apropiado. Deberían incluir toda responsabilidad general para implantar o mantener la política de seguridad, así como cualquier responsabilidad específica para la protección de activos particulares y la ejecución de procesos o actividades particulares de seguridad.

6.1.2 Selección y política de personal

Deberían realizarse comprobaciones en la plantilla fija en el momento de la solicitud de trabajo. Esto debería incluir controles como los siguientes:

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).

La organización debería realizar también una comprobación del crédito 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. Esta comprobación debería repetirse periódicamente para puestos de alta responsabilidad.
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.

La gerencia debería evaluar la supervisión que requiere el personal nuevo e inexperto con acceso autorizado a sistemas sensibles. El trabajo de todo el personal debería revisarse periódicamente y aprobarse sus procedimientos por personal de más categoría.

Los directivos deberían conocer qué circunstancias privadas de su personal pueden afectar a su trabajo. Los problemas personales o financieros, los cambios de su comportamiento o estilo de vida, las ausencias recurrentes y la depresión o el estrés evidentes podrían llevar a fraudes, robos, errores u otras implicaciones de seguridad. Esta información debería manejarse de acuerdo con la legislación correspondiente.

6.1.3 Acuerdos de confidencialidad

Se usan acuerdos de confidencialidad o no divulgación para notificar qué información es secreta o confidencial. Los empleados normalmente deberían firmar dicha cláusula como parte de sus términos o condiciones iniciales de trabajo.

La organización debería requerir la firma de un acuerdo de confidencialidad a los recursos humanos externos o a los usuarios de terceros no cubiertos por un contrato de trabajo (que contiene cláusulas de confidencialidad) antes de su acceso a los recursos de tratamiento de información.

Las cláusulas de confidencialidad deberían revisarse cuando cambien los términos del empleo o contrato, especialmente cuando los empleados dejen la organización o sus contratos terminen.

6.1.4 Términos y condiciones de la relación laboral

Los términos y las condiciones de empleo deberían establecer la responsabilidad del empleado en materia de seguridad de la información. Dicha responsabilidad debería continuar durante un periodo definido tras la finalización del contrato. Debería incluirse qué hacer si el empleado incumple los requisitos de seguridad.

Deberían aclararse e incluirse en los términos y las condiciones de empleo las responsabilidades y obligaciones legales por ejemplo respecto a las leyes de propiedad intelectual o de protección de datos. También debería incluirse la responsabilidad por la clasificación y gestión de los datos del empleador. Los términos y las condiciones del contrato deberían establecer, cuando proceda, que dichas responsabilidades se extienden fuera del ámbito de la organización y de las horas normales de trabajo, por ejemplo, en el caso del trabajo en casa (véanse también los incisos 7.2.5 y 9.8.1).

6.2 Formación de usuarios

OBJETIVO: Asegurar que los usuarios son 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.

Los usuarios deberían recibir formación en procedimientos de seguridad y en el uso correcto de los recursos de tratamiento de información para minimizar los posibles riesgos en la seguridad.

6.2.1 Formación y capacitación en seguridad de la información

Todos los empleados de la organización y los usuarios de terceros, cuando corresponde, deberían recibir la formación adecuada y actualizaciones regulares en las políticas y procedimientos de la organización. Incluyendo requisitos de seguridad, responsabilidades legales y otros controles del negocio, así como prácticas en el uso correcto de los recursos de tratamiento de información (procedimientos de conexión (log-on) , uso de paquetes de software, etc.), antes de obtener acceso a la información o los servicios.

6.3 Respuesta ante incidencias y malos funcionamientos de la seguridad

OBJETIVO: Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Debería informarse de las incidencias que afecten a la seguridad de la información por los canales de la organización adecuados, lo más rápidamente posible.

Todos los empleados y contratados deberían conocer los procedimientos para informar de los distintos tipos de incidencias (fallo de seguridad, amenaza, debilidad o mal funcionamiento) que puedan tener impacto en la seguridad de los activos de la organización. Se les debería, pedir que informen al punto de contacto designado, de toda incidencia observada o sospechada, tan rápido como sea posible. La organización debería formalizar un proceso disciplinario para los empleados que cometan infracciones en materia de seguridad. Para poder gestionar las incidencias adecuadamente, se necesitan recoger evidencias de las incidencias tan pronto como sea posible (véase el inciso 12.1.7).

6.3.1 Comunicación de las incidencias de seguridad

Debería informarse de las incidencias que afecten a la seguridad por los canales de gestión adecuados lo más rápidamente posible.

Se debería formalizar un procedimiento de información, junto al procedimiento de respuesta a la incidencia, que establezca la acción a adoptar cuando se reciba una notificación de incidencia. Todos los empleados y contratados deberían conocer el procedimiento para notificar las incidencias de seguridad e informar de ellas, tan rápido como sea posible. Se deberían implantar procesos adecuados de respuesta que aseguren la notificación al informante de la incidencia y de la resolución y cierre de la misma. Estas incidencias pueden usarse para prácticas de concientización (véase el inciso 6.2), como ejemplos de lo qué hubiera podido suceder, de cómo responder ante ellas y de cómo evitarlas en el futuro (véase también el inciso 12.1.7).

6.3.2 Comunicación de las debilidades de seguridad

Se debería requerir a los usuarios de los servicios de información que detecten e informen acerca de toda debilidad - o amenaza **-** observada o sospechada, respecto a la seguridad de los sistemas o servicios. Deberían informar sobre estos asuntos lo más pronto posible a su propia gerencia o directamente al proveedor del servicio. Se debería informar a los usuarios que no es conveniente que traten de probar las sospechas de debilidad en ninguna circunstancia. Esto es para su propia protección, ya que dicha prueba de las debilidades podría interpretarse como un posible mal uso del sistema.

6.3.3 Comunicación de los fallos del software.

Se deberían establecer procedimientos para comunicar los fallos del software. Se deberían considerar las siguientes acciones:

a) Se deberían anotar los síntomas del problema y todo mensaje que aparezca en pantalla.

b) Se debería aislar el sistema, si es posible, y pararse su uso, alertando inmediatamente al contacto de soporte adecuado. Si hay que examinar el equipo, se debería desconectar de las redes de la organización antes de volver a conectarlo. No se deberían transferir discos a otros computadores.

c) Se debería informar inmediatamente de la situación al gerente de seguridad de la información.

Los usuarios no deberían intentar retirar el software sospechoso salvo autorización expresa. La recuperación se debería realizar por personal experimentado y debidamente formado.

6.3.4 Aprendiendo de las incidencias

Se deberían instalar mecanismos para cuantificar y monitorear los tipos, volúmenes y costos de las incidencias y malos funcionamientos. Esta información se debería usar para identificar aquellos que se produzcan con mayor frecuencia o tengan un fuerte impacto. Esto puede indicar la necesidad de mejora o ampliación de controles para limitar la frecuencia, daño y costo de futuras ocurrencias, o bien para tenerlas en cuenta en el proceso de revisión de la política de seguridad (véase el inciso 3.1.2).

6.3.5 Procedimiento disciplinario

Debería formalizarse un procedimiento disciplinario para los empleados que violen las políticas y procedimientos de seguridad de la organización (véanse los incisos 6.1.4 y 12.1.7 para la retención de pruebas). Dicho procedimiento puede actuar como disuasor a empleados que de otra forma puedan inclinarse a desatender los procedimientos de seguridad. Asimismo debería asegurar un tratamiento adecuado y justo para empleados sospechosos de cometer violaciones serias o continuadas de los procedimientos de seguridad.

7. SEGURIDAD FÍSICA Y DEL ENTORNO

7.1 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. Se recomienda una política de puesto de trabajo despejado, y bloqueo de pantalla para reducir el riesgo de accesos no autorizados o de daños a documentos, medios y recursos de tratamiento de información.

7.1.1 Perímetro de seguridad física

La protección física puede lograrse creando una serie de barreras físicas en torno a los locales de la organización y a los recursos de tratamiento de la información. Cada barrera establece un perímetro de seguridad que aumenta la protección total. Las organizaciones deberían usar perímetros de seguridad para proteger áreas que contienen recursos de tratamiento de información (véase el inciso 7.1.3). Un perímetro de seguridad es algo que constituye una barrera, por ejemplo, un muro, una puerta de entrada controlada por tarjeta o un puesto manual de recepción. La colocación y resistencia de cada barrera depende de los resultados de una evaluación del riesgo.

Las siguientes pautas y controles deberían ser consideradas e implantadas donde sea apropiado:

a) El perímetro de seguridad debería estar claramente definido.

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.

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 (como la causada por incendios o inundaciones).

e) Todas las puertas para incendios del perímetro de seguridad deberían tener alarma y cierre automático.

7.1.2 Controles físicos de entradas

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

a) Las visitas a las áreas seguras se deberían supervisar u ordenar y registrarse su 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 deberían revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

7.1.3 Seguridad de oficinas, despachos y recursos

Un área segura puede ser una oficina cerrada, o varios despachos dentro de un perímetro de seguridad física, que puedan cerrarse y contener armarios o cajas de seguridad con cierre. La selección y el diseño de un área de seguridad tendrá en cuenta la posibilidad de daños por incendio, inundación, explosión, disturbio y otras formas de desastres naturales o provocados, así como las reglas y normas apropiadas sobre salud y sanidad. Se deberían considerar también las amenazas que procedan de otros lugares vecinos, por ejemplo, inundaciones provocadas en otras áreas.

Los siguientes controles deberían ser considerados:

a) Los recursos críticos deberían situarse fuera de áreas de acceso público.

b) Los edificios deberían ser discretos y dar mínimas indicaciones de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información.

c) Las funciones y equipos de soporte, por ejemplo fotocopiadoras, faxes, etc. se deberían situar adecuadamente en el área de seguridad para evitar demandas de acceso que puedan debilitar la seguridad de la información.

d) Las ventanas y puertas deberían permanecer cerradas cuando la instalación esté vacía. Se debería tener protección externa en las ventanas, sobre todo en las de la planta baja.

e) Se deberían instalar sistemas de detección de intrusos y probarse regularmente para cubrir todas las puertas externas y las ventanas accesibles. Las alarmas de espacios no ocupados deberían estar activadas permanentemente. También se deberían cubrir otras áreas como las salas de cómputo o de comunicaciones.
f) Los recursos de tratamiento de información gestionados por la organización se deberían separar físicamente de los gestionados por terceros.

g) El público no debería acceder automáticamente a los ambientes o directorios de información personal de la organización que identifiquen lugares con recursos de tratamiento de información sensible.

h) 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.

i) 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.

7.1.4 El trabajo en las áreas seguras

Se deberían requerir controles y normas adicionales para asegurar más un área de seguridad; entre otros, controles para actividades de terceros o tareas de su personal que se desarrollen en el área segura. Los controles siguientes deberían ser considerados:

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) El personal de servicios de apoyo de terceros, debidamente autorizado, sólo debería acceder a las áreas de seguridad o a recursos de tratamiento de información sensible cuando sea requerido y su acceso se supervisará. Se pueden necesitar barreras y perímetros adicionales entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad.

e) No se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.

7.1.5 Áreas aisladas de carga y descarga

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. Los requisitos de seguridad para dichas áreas se deberían determinar mediante una evaluación del riesgo. Se deberían considerar los siguientes controles:

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

b) El área 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 (véase el inciso 7.2.1.d) antes de llevarlo a su lugar de utilización.

e) El material entrante se debería registrar, si procede, (véase el inciso 5.1) al entrar en el lugar.

7.2 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 y riesgos del entorno para reducir el riesgo de accesos no autorizados a los datos y protegerlo contra pérdidas o daños. 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.

7.2.1 Instalación y protección de equipos

El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. Se deberían considerar los siguientes controles:

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 otros 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) para minimizar los riesgos de posibles amenazas como las siguientes:

1) robo;

2) incendio;

3) explosivos;

4) humo;

5) agua (o fallo de suministro);

6) polvo;

7) vibraciones;

8) agentes químicos;

9) interferencias en el suministro eléctrico;

10) radiaciones electromagnéticas.

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 que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información.

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

h) Se deberían considerar los impactos de desastres que puedan ocurrir en lugares próximos, tanto vertical como horizontalmente, por ejemplo el incendio en el edificio vecino, fugas de agua en pisos superiores o una explosión en la calle.

7.2.2 Suministro eléctrico

Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas. Debería garantizarse un suministro eléctrico adecuado que cumpla con las especificaciones de los fabricantes de equipos.

Las siguientes opciones aseguran la continuidad de suministro:

a) redes múltiples de alimentación para evitar el fallo puntual de suministro;

b) Sistemas de Alimentación Ininterrumpida (U.P.S.);

c) generador de respaldo (grupo electrógeno).

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. Los equipos de UPS se deberían revisar regularmente para asegurar que tienen la capacidad adecuada y que están probados de acuerdo con las recomendaciones del fabricante.

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.

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. Se deberían instalar en todos los edificios, así como en todas las líneas exteriores de comunicaciones, sistemas y filtros de protección para rayos.

7.2.3 Seguridad del cableado

Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información. Se deberían considerar los siguientes controles:

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) 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) inicialización de barreras contra el enganche a los cables de dispositivos no autorizados.

7.2.4 Mantenimiento de equipos

Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. Los controles siguientes 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 deberían adoptar las medidas adecuadas cuando se envíen los equipos fuera de las instalaciones, para su mantenimiento (véase también el inciso 7.2.6 respecto a datos destruidos, borrados o sobrescritos). Se deberían cumplir todos los requisitos impuestos por las políticas de los seguros.

7.2.5 Seguridad de equipos fuera de los locales de la organización

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. Se debería proporcionar una seguridad equivalente a la de los equipos instalados dentro para el mismo propósito, teniendo en cuenta los riesgos de trabajar fuera de dichos locales. El equipo de tratamiento de información comprende todo tipo de computadores personales, agendas electrónicas (PDAS), teléfonos móviles, documentos u otros, que se lleven al domicilio o fuera del lugar habitual de trabajo. Se deberían considerar las siguientes indicaciones:

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.

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. Puede encontrarse en el inciso 9.8.1 más información sobre otros aspectos de la protección de equipos móviles.

7.2.6 Seguridad en el reuso o eliminación de equipos

La información pueden exponerse a riesgo si el reuso o eliminación de los equipos se realiza sin precaución (véase también el inciso 8.6.4). Los dispositivos de almacenamiento con información sensible se deberían destruir físicamente o sobre escribirse de manera segura y no simplemente usando la función normalizada de borrado (delete).

Todos los elementos del equipo que contengan dispositivos de almacenamiento de datos, por ejemplo discos duros fijos, deberían comprobarse antes de su reuso o eliminación para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito. Los dispositivos de almacenamiento dañados que contengan datos sensibles pueden requerir una minuciosa evaluación del riesgo para determinar si deberían destruirse, repararse o eliminarse.

7.3 Controles generales

OBJETIVO: Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

La información y los recursos de tratamiento de información deberían estar protegidos de su difusión, modificación no autorizada o robo; se deberían instalar medidas y controles para minimizar las pérdidas y los daños.
Se consideran procedimientos de utilización y almacenamiento descritos en el inciso 8.6.3.

7.3.1 Política de puesto de trabajo despejado y bloqueo de pantalla

Las organizaciones deberían adoptar una política de puesto de trabajo despejado de papeles y medios de almacenamiento removibles y una política de bloqueo de pantalla para los recursos de tratamiento de información con objeto de reducir los riesgos de acceso no

autorizado, pérdidas o daños de la información dentro o fuera del horario normal de trabajo. Dicha política debería tener en cuenta la clasificación de seguridad (véase el inciso 5.2), sus riesgos correspondientes y los aspectos culturales de la organización.

La información que se deja sobre las mesas también puede dañarse o destruirse en un desastre como un incendio, una inundación o una explosión.

Se deberían considerar los siguientes controles:

a) Cuando no se estén usando, los papeles y los medios informáticos se deberían guardar en locales cerrados y/o en los tipos de mobiliario de seguridad adecuados, especialmente fuera de las horas de trabajo.

b) Cuando no se esté usando, la información sensible o crítica para la organización se debería guardar fuera (lo mejor en un armario o un lugar resistente al fuego), especialmente cuando el despacho esté desocupado.

c) Los computadores personales y terminales no se deberían dejar desatendidos una vez completados los procesos de identificación y autenticación de usuario, ni las impresoras encendidas, y deberían estar protegidos por cierres, contraseñas u otras medidas cuando no se estén utilizando.

d) Se deberían proteger los puntos de entrada y salida de correo así como las máquinas de fax y télex no atendidas.

e) Las fotocopiadoras se deberían cerrar (o protegerse por medios similares contra su uso no autorizado) fuera de las horas de trabajo.

f) Se debería sacar inmediatamente de las impresoras la información sensible o clasificada.

7.3.2 Extracción de pertenencias

No se deberían sacar de las instalaciones sin autorización los equipos, la información o el software. Cuando haya necesidad de sacar los equipos, se debería registrar su salida y su retorno. Se deberían hacer controles puntuales de existencias para detectar sustracciones, de las que se advertirá al personal.

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES

8.1 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 (véase el inciso 8.1.4), cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

8.1.1 Documentación de procedimientos operativos

Se deberían documentar y mantener los procedimientos de operación identificados por la política de seguridad: Estos procedimientos, se deberían tratar como documentos formales y sus cambios han de autorizarse por la gerencia.

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) 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;

c) 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 9.5.5.);

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

e) 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;

f) el rearranque del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema.

También se deberían preparar procedimientos documentados para las actividades de administración del sistema asociadas a los recursos de tratamiento y comunicación de la información, como los procedimientos de arranque y cierre de los computadores, los datos de respaldo el mantenimiento de los equipos, o la gestión de la seguridad de la sala de cómputo y de la utilización del correo.

8.1.2 Control de cambios operacionales

Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. 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. Los programas operativos deberían estar sujetos a un control estricto de cambios. Cuando se cambien los programas se debería conservar un registro de auditoria conteniendo toda la información importante. Se deberían integrar, siempre que sea posible, los procedimientos de control de los cambios operacionales y aplicativos (véase también el inciso 10.5.1). En particular se deberían considerar los siguientes controles y medidas:

a) la identificación y registro de cambios significativos;

b) la evaluación del posible impacto de los cambios;

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

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

e) procedimientos que identifiquen las responsabilidades de abortar y recuperar los cambios sin éxito.

8.1.3 Procedimientos de gestión de incidencias

Se deberían establecer responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a las incidencias en materia de seguridad (véase también el inciso 6.3.1). Se deberían considerar los siguientes controles:

a) Se deberían establecer procedimientos para cubrir todos los tipos posibles de incidencias de seguridad, incluyendo:

1) fallos del sistema de información y pérdidas de servicio;

2) denegación de servicio;

3) errores que resultan de datos del negocio inexactos o incompletos;

4) violaciones de confidencialidad.

b) Estos procedimientos deberían cubrir, además de los planes de contingencia normales, diseñados para recuperar sistemas o servicios tan rápidamente como sea posible (véase también el inciso 6.3.4):

1) el análisis e identificación de la causa de la incidencia;

2) la planificación e implantación de medidas para evitar su repetición, si fuera necesario;

3) la recogida de pistas de auditoría y otras evidencias similares;

4) la comunicación con los afectados o implicados en la recuperación de la incidencia;
5) la comunicación de las acciones realizadas a la autoridad apropiada.

c) Las pistas de auditoría y evidencias similares se deberían recoger y asegurar debidamente (véase el inciso 12.1.7) para:

1) el análisis interno del problema;

2) el uso de la evidencia como prueba de posible incumplimiento de contrato o de un requisito reglamentario y en el caso de procedimientos civiles o penales en que se estuviera incurriendo, por ejemplo, por la mala utilización de los computadores o el incumplimiento de la legislación de protección de datos;

3) la negociación de compensaciones con los proveedores de software y servicios.

d) La acción para recuperarse de los efectos de los fallos de seguridad y corregir los fallos del sistema debería controlarse cuidadosa y formalmente. Estos procedimientos deberían asegurar que:

1) sólo se permite el acceso a sistemas y datos al personal claramente identificado y autorizado (véase también el inciso 4.2.2 para acceso de terceros);

2) se documentan detalladamente todas las acciones realizadas por emergencias;

3) se traslada cada acción de emergencia a la gerencia y se revisa de forma ordenada;

4) se confirma lo antes posible la integridad de los sistemas de la organización y las medidas de control de seguridad.

8.1.4 Segregación de tareas

La segregación de tareas es un método para reducir el riesgo de mal uso accidental o deliberado de un sistema. Se debería considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de mal uso de la información o los servicios.

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 auditoría y la supervisión de la gestión. Es importante que la auditoría de seguridad permanezca independiente.

Se debería vigilar que ninguna persona pueda realizar por sí sola ningún fraude en áreas de responsabilidad única que no sea detectable. El comienzo de un evento se debería separar de su autorización.

Se deberían considerar los siguientes controles:

a) Es importante segregar las actividades que requieran confabulación para realizar un fraude, por ejemplo, lanzar una orden de compra y verificar la recepción de la mercancía.

b) Si hay riesgo de confabulación, se diseñarán controles que impliquen a dos o más personas, reduciendo así la posibilidad de conspiración.

8.1.5 Separación de los recursos para desarrollo y para producción

La separación de los recursos para desarrollo, prueba y producción es importante para conseguir la segregación de las responsabilidades implicadas. Se deberían definir y documentar las reglas para transferir el software del entorno de desarrollo al de producción.

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. Se debería valorar qué nivel de separación es necesario entre los entornos de desarrollo, prueba y producción para evitar problemas operacionales. Se debería implantar también una separación similar entre las funciones de desarrollo y prueba. 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. Deberían considerarse los controles y medidas siguientes:

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

b) Las tareas de desarrollo y de prueba deberían separarse tanto como sea posible.

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

d) Se usarán diferentes procedimientos de conexión 'log-on' en los sistemas de producción y prueba para reducir el riesgo de confusión. Se debería animar a los usuarios para que empleen contraseñas diferentes para estos dos sistemas y los menús deberían exhibir los mensajes de identificación apropiados.

e) El equipo de desarrollo debería acceder a las contraseñas de producción, sólo donde se hayan establecido los controles que requieran contraseñas para soporte del sistema de producción. Dichos controles deberían asegurar que se cambiarán las contraseñas después de usarlas.

8.1.6 Gestión de servicios externos

La contratación de un proveedor externo para gestionar los recursos de tratamiento de información puede introducir posibles vulnerabilidades, como la posibilidad de daño, pérdida o comprometer los datos en el local del contratista. Se deberían identificar estos riesgos de antemano e incorporarse al contrato las medidas de seguridad apropiadas de acuerdo con el contratista (véanse también los incisos 4.2.2 y 4.3 sobre contratos con terceros que impliquen el acceso a recursos organizativos y contratos de outsourcing).

Se deberían tratan cuestiones específicas como:

a) la identificación de las aplicaciones sensibles o críticas que es mejor retener en la organización;

b) la aprobación por los propietarios de la aplicación;

c) las implicaciones para los planes de continuidad del negocio;

d) las normas de seguridad a especificar y el proceso para medir su conformidad;

e) la adjudicación de responsabilidades y procedimientos especiales para monitorear eficazmente todas las actividades importantes de seguridad;

f) responsabilidades y procedimientos para informar y manejar las incidencias sobre seguridad (véase el inciso 8.1.3).

8.2 Planificación y aceptación del sistema

OBJETIVO: Minimizar el riesgo de fallos de los sistemas.

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. Se deberían coordinar y revisar regularmente los requisitos de recuperación de caídas de los servicios que soportan aplicaciones múltiples.

8.2.1 Planificación de la capacidad

Deberían comprobarse las demandas actuales y las proyecciones de los requisitos futuros de capacidad para asegurar la disponibilidad de capacidad de procesamiento y almacenamiento adecuados. Estas 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.

Los computadores corporativos requieren una atención particular, pues conseguir con ellos mayor capacidad tiene un costo y tiempo muy superiores. Sus administradores deberían monitorear el uso de los recursos críticos del sistema, incluyendo los procesadores, el almacenamiento principal y el de archivos, las impresoras, otros dispositivos de salida y los sistemas de comunicaciones. 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.

8.2.2 Aceptación del sistema

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. Los administradores se deberían asegurar que los requisitos y criterios de aceptación de los nuevos sistemas estén claramente definidos, acordados, documentados y probados. Se deberían considerar los siguientes controles:

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.

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.

8.3 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” (véase también el inciso 10.5.4) 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. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en los computadores personales.

8.3.1 Medidas y controles contra software malicioso

Se deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios. 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 12.1.2.2);

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 (véase también el inciso 10.5, especialmente los incisos 10.5.4 y 10.5.5);

c) 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;

d) 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;

e) 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;

f) 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;

g) 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 6.3 y 8.1.3);

h) 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 11);

i) 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.

Estos controles y medidas son especialmente importantes en los servidores que soportan un gran número de estaciones de trabajo.

8.4 Gestión interna 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 11.1) haciendo copias de seguridad, ensayando su oportuna recuperación, registrando eventos o fallos y monitoreando el entorno de los equipos cuando proceda.

8.4.1 Recuperación de la información

Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software. 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. Se deberían comprobar regularmente los procedimientos de respaldo para sistemas individuales para asegurar que cumplen los requisitos de los planes de continuidad del negocio (véase el capítulo 11). Se deberían considerar los siguientes controles:

a) 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, a una distancia suficiente para evitar todo daño por un desastre en el local principal. Se retendrán como mínimo tres generaciones o ciclos de información de respaldo para las aplicaciones importantes del negocio.

b) Se debería dar a la información de respaldo un nivel adecuado de protección física y del entorno (véase el capítulo 7), 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.

c) 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.

d) 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.

Se debería determinar el periodo de retención de la información esencial del negocio, así como los requisitos de archivo de copias a retener permanentemente (véase el inciso 12.1.3).

8.4.2 Diarios de operación

El personal de operaciones debería mantener un diario (log), de sus actividades. Los diarios deberían incluir, según sea más adecuado:

a) los tiempos de arranque y cierre del sistema;

b) los errores del sistema y las acciones adoptadas para su corrección;
c) la confirmación de la utilización correcta de los archivos de datos y los resultados;

d) el nombre de quién registra la entrada en el diario.

Los diarios de los operadores deberían estar sujetos a comprobaciones regulares e independientes respecto a los procedimientos de operación.

8.4.3 Registro de fallos

Se debería informar sobre los fallos y las acciones adoptadas para corregirlos. Se deberían registrar los fallos comunicados por los usuarios en relación a problemas en los sistemas de tratamiento de información o de comunicaciones. Deberían existir reglas precisas para gestionar los fallos registrados, incluyendo:

a) la revisión de los registros de fallos para asegurar que se han resuelto satisfactoriamente;

b) la revisión de las medidas correctivas para asegurar que los controles no se han visto comprometidos y que la acción adoptada está debidamente autorizada.

8.5 Gestión de 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.

8.5.1 Controles de red

Se requieren una serie de controles para alcanzar y mantener la seguridad en las redes de computadores.

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 8.1.4).

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 9.4 y 10.3). También se deberían requerir controles y medidas especiales para mantener la disponibilidad de los servicios de las redes y de los computadores conectados.

d) 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.

8.6 Utilización y seguridad de los medios de información

OBJETIVO: Evitar daños a los activos e interrupciones de las actividades de la organización.

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, robo y acceso no autorizado.

8.6.1 Gestión de medios removibles

Debería haber procedimientos para la gestión de los medios informáticos removibles como cintas, discos o resultados impresos. Se deberían considerar los siguientes controles:

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

b) Todo medio desechado por la organización debería requerir autorización y se debería guardar registro de dicha remoción para guardar una pista de auditoría (véase el inciso 8.7.2).

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

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

8.6.2 Eliminación de medios

Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más. Podría filtrarse a personas externas información sensible si los medios se eliminan sin precauciones. Se deberían establecer procedimientos formales para minimizar este riesgo con la eliminación segura de los medios. Se deberían considerar los siguientes controles:

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) La lista siguiente identifica qué elementos requieren una eliminación segura:

1) documentos sobre papel;

2) registros de voz;

3) papel carbón;

4) informes;

5) cintas de impresora de un solo uso;

6) cintas magnéticas;

7) discos extraíbles;

8) medios de almacenamiento óptico, incluidos los de distribución de software de fabricantes;

9) listados de programas;

10) datos de pruebas;
11) documentación de los sistemas.

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 auditoría.

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.

8.6.3 Procedimientos de manipulación de la información

Se deberían establecer procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación (véase el inciso 5.2) para protegerla de su mal uso o divulgación no autorizada, y de acuerdo con su medio en documentos, sistemas informáticos, redes, computadores portátiles, correo, correo de voz, transmisiones de voz en general, multimedia, servicios y equipos postales, máquinas de fax y otros elementos sensibles como cheques en blanco o facturas. Se deberían considerar los controles siguientes (véanse también los incisos 5.2 y 8.7.2):

a) etiquetado en la administración de todos los medios (véase también el inciso 8.7.2);

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.

8.6.4 Seguridad de la documentación de sistemas

La documentación de sistemas puede contener una variedad de información sensible, por ejemplo, las descripciones de los tratamientos de las aplicaciones, procedimientos, estructuras de datos, procesos de autorización (véase también el inciso 9.1). Para proteger la documentación de sistemas de accesos no autorizados se deberían considerar los controles y medidas siguientes:

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.

8.7 Intercambio de información y software

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

Se deberían controlar los intercambios de información y software entre organizaciones, que deberían cumplir con toda la legislación correspondiente (véase el capítulo 12).

Se deberían realizar los intercambios sobre la base de acuerdos formales. Se deberían establecer procedimientos y normas para proteger los medios en tránsito. Se considerarán las implicancias de seguridad asociadas al comercio, correo e intercambio electrónico de datos (EDI), así como los requisitos para las medidas y controles de seguridad.

8.7.1 Acuerdos para intercambio de información y software

Se deberían establecer acuerdos, algunos formales, incluyendo los de custodia del software, si procede, para los intercambios (sean manuales o electrónicos) de información y software entre organizaciones. El nivel de seguridad recogido en los acuerdos debería reflejar la criticidad de la información implicada. Los acuerdos en las condiciones de seguridad deberían considerar:

a) la responsabilidad de administrar el control y notificación de la transmisión, su despacho y recepción;

b) los procedimientos para notificar el envío, transmisión, despacho y recepción;
c) las mínimas normas técnicas para el empaquetado y transmisión;

d) las normas de identificación del mensajero;

e) las responsabilidades y obligaciones en caso de pérdida de datos;

f) el uso de un sistema acordado de etiquetado para la información sensible o crítica, asegurando que el significado de las etiquetas se comprende inmediatamente y que la información está debidamente protegida;

g) la propiedad de la información, y del software y las responsabilidades de protección de los datos, el cumplimiento de la propiedad intelectual del software y consideraciones semejantes (véanse los incisos 12.1.2 y 12.1.4);

h) las normas técnicas para grabación y lectura de información y software;

i) toda medida y control especiales requeridos para proteger los elementos sensibles, como las claves criptográficas (véase el inciso 10.3.5).

8.7.2 Seguridad de medios en tránsito

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. Debería convenirse entre las gerencias una lista de mensajeros autorizados y un procedimiento para comprobar la identificación de los utilizados.
b) 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.

c) 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;

5) uso de firmas digitales y de cifrado para hacer confidencial el contenido (véase el inciso 10.3).

8.7.3 Seguridad en comercio electrónico

El comercio electrónico puede implicar el uso de intercambio electrónico de datos (EDI), de correo electrónico y transacciones en línea a través de redes públicas como Internet. El comercio electrónico es vulnerable a ciertos tipos de amenazas que llevan a actividades fraudulentas, litigios contractuales y divulgación o modificación de la información. Se deberían aplicar controles y medidas para proteger al comercio electrónico de dichas amenazas. Las consideraciones de seguridad para el comercio electrónico deberían incluir los siguientes controles y medidas:

a) Autenticación ¿Qué nivel de confianza deberían requerir comprador y vendedor en la identidad que afirma el otro?

b) Autorización. ¿Quién está autorizado para establecer los precios y redactar o firmar los documentos comerciales clave? ¿Cómo puede conocer esto el socio comercial?

c) Procesos de oferta y contratación. ¿Cuáles son los requisitos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y del no repudio de los contratos?

d) Información de precios. ¿Qué nivel de confianza puede tenerse en la integridad de la lista de precios publicada y en la confidencialidad de los acuerdos secretos sobre descuentos?

e) Transacciones de pedidos. ¿Cómo se logra la confidencialidad e integridad de los detalles del pedido, dirección de pago, domicilio de entrega y confirmación de recepción?

f) Verificación. ¿Qué grado de verificación es apropiado para comprobar la información del pago suministrada por el cliente?

g) Satisfacción del pago. ¿Cuál es la forma de pago más apropiada para protegerse contra el fraude?

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

i) Deuda. ¿Quién soporta el riesgo de las posibles transacciones fraudulentas?

Muchas de estas consideraciones pueden resolverse aplicando las técnicas de cifrado reseñadas en el inciso 10.3, teniendo en cuenta el cumplimiento de los requisitos legales (véase 12.1 y sobre todo 12.1.6 para legislación sobre criptografía).

Los acuerdos sobre comercio electrónico entre las partes comerciales se deberían reseñar en un documento que consigne los términos acordados por ambas partes, incluyendo

detalles sobre las autorizaciones (véase el punto b anterior). Pueden ser necesarios otros acuerdos con los proveedores de servicios de información y redes de valor agregado.

Los sistemas públicos de comercio deberían publicar a los clientes sus términos de negocio.

Se debería considerar la capacidad de recuperación, ante un ataque, del servidor usado para comercio electrónico y los riesgos que implican las interconexiones por red que requiere su implantación (véase el inciso 9.4.7).

8.7.4 Seguridad del correo electrónico

8.7.4.1 Riesgos de seguridad

El correo electrónico se está usando para comunicaciones empresariales, reemplazando formas tradicionales de comunicación como el telex y las cartas. El correo electrónico tiene ciertas características diferentes de las formas tradicionales de comunicaciones de negocios, como su velocidad, la estructura del mensaje, el grado de formalización y la vulnerabilidad a las acciones no autorizadas. Se debería considerar la necesidad de controles y medidas para reducir los riesgos que implique el correo electrónico. Riesgos que incluyen:

a) la vulnerabilidad de los mensajes a interceptación, modificación o denegación del servicio;

b) la vulnerabilidad al error (por ejemplo dirección incorrecta o inexistente), la fiabilidad en general y la disponibilidad del servicio;

c) el impacto de un cambio de soporte de comunicación en los procesos del negocio por ejemplo el efecto de un aumento de velocidad del despacho o del envío entre personas en lugar de entre organizaciones;

d) consideraciones legales como la posible necesidad de prueba del origen, despacho, entrega y aceptación;

e) las implicaciones de la publicación del directorio de personas accesible desde el exterior;

f) el control del acceso de usuarios remotos a las cuentas del correo electrónico.

8.7.4.2 Política de correo electrónico

Las organizaciones deberían diseñar una política clara sobre el uso del correo electrónico, incluyendo:

a) los ataques al correo electrónico, por ejemplo, virus o interceptación;

b) la protección de los archivos adjuntos;

c) directrices sobre cuando usar o no el correo electrónico;

d) la responsabilidad del empleado de no comprometer a la organización, por ejemplo, si realiza difamaciones, hostigamiento o compras no autorizadas con ayuda del correo electrónico;

e) el uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (véase el inciso 10.3);

f) la retención de los mensajes que podrían descubrirse en caso de litigio, si se almacenaran;

g) controles y medidas adicionales para examinar los mensajes no autenticados.

8.7.5 Seguridad de los sistemas ofimáticos

Se deberían preparar e implantar políticas y directrices para controlar los riesgos del negocio asociados con los sistemas ofimáticos. Estos proporcionan oportunidades para difundir más rápidamente y para compartir la información del negocio usando una combinación de documentos, computadores, computadores portátiles y comunicaciones móviles, correo escrito y de voz, comunicaciones de voz en general, multimedia, servicios y recursos postales y máquinas de fax.

Se deberían considerar las implicaciones en el negocio y en la seguridad de interconectar estos recursos, incluyendo:

a) las vulnerabilidades de la información en los sistemas ofimáticos, por ejemplo, el registro de las llamadas telefónicas, su confidencialidad, el almacenamiento de faxes, la apertura del correo y su distribución;

b) una política y medidas apropiadas para manejar información compartida, por ejemplo, el uso de tableros de anuncios electrónicos corporativos (véase el inciso 9.1);

c) la exclusión de categorías de información sensible del negocio si el sistema no proporciona un nivel apropiado de protección (véase el inciso 5.2);

d) la restricción del acceso a la información diaria a determinadas personas (por ejemplo a ejecutivos que trabajen en proyectos sensibles);

e) la conveniencia (o no) de que el sistema soporte aplicaciones del negocio, como la comunicación de pedidos o autorizaciones;

f) las categorías del personal, contratistas o socios del negocio que tengan permiso para usar el sistema y los sitios desde donde se pueda acceder (véase el inciso 4.2);

g) la restricción de recursos seleccionados en función a categorías específicas de usuarios;

h) la identificación del 'status' de los usuarios, por ejemplo, empleados de la organización o contratistas en directorios corporativos para beneficio de otros usuarios;

i) la retención y respaldo de la información contenida en el sistema (véanse los incisos 12.1.3. y 8.4.1);

j) los requisitos y disposiciones para recuperar caídas (véase el inciso 11.1).

8.7.6 Sistemas públicamente disponibles

Se debería cuidar la protección de la integridad de la información publicada electrónicamente para evitar la modificación no autorizada que pueda dañar la reputación de la organización que la publica. La información en un sistema disponible públicamente, por ejemplo, la información en un servidor Web accesible vía Internet, tendrá que cumplir las leyes, regulaciones y reglas de la jurisdicción donde se sitúa el sistema o donde se realiza la acción comercial. Debería haber un proceso de autorización formal antes de que la información esté disponible públicamente.

El software, datos y otra información que requiera un alto nivel de integridad y que estén disponibles públicamente deberían protegerse por mecanismos adecuados, por ejemplo, firmas digitales (véase el inciso 10.3.3). Los sistemas disponibles públicamente, en especial los que permiten la realimentación directa de información, se deberían controlar cuidadosamente para que:

a) la información se obtenga de acuerdo con la legislación de protección de datos (véase el inciso 12.1.4);

b) la entrada de información y su tratamiento por el sistema de publicación se procesarán completa y exactamente en forma oportuna;

c) la información sensible se protegerá durante su recojo y almacenamiento;

d) el acceso al sistema de publicación no permitirá el acceso no autorizado a las redes a las que está conectado.

8.7.7 Otras formas de intercambio de información

Se deberían implementar procedimientos y controles para la protección del intercambio de información cuando se usan recursos de comunicación de voz, facsímil y vídeo.

La información podría tener vulnerabilidades por falta de cuidado, de políticas o de procedimientos de uso de dichos recursos, por ejemplo, por un tono elevado de los contestadores automáticos o del teléfono móvil en un sitio público o por el acceso no autorizado a sistemas de mensajes o por el envío de facsímiles a una dirección equivocada.

Las operaciones de la organización pueden detenerse y la información verse comprometida si los recursos de comunicación fallan, se sobrecargan o se interrumpen (véase el inciso 7.2 y el capítulo 11). La información también puede ser vulnerable al acceso por usuarios no autorizados (véase el capítulo 9).

Se debería establecer una política clara de procedimientos que se espera sea seguida por el personal para usar recursos de comunicación de voz, facsímil y vídeo. Esto debería incluir:

a) recordar al personal qué debería tomar las precauciones adecuadas, por ejemplo, no revelar información sensible para evitar la escucha o interceptación de su llamada por:

1) personas de su vecindad próxima sobre todo cuando se usa un teléfono móvil;

2) intervención de comunicaciones o espionaje a través del acceso físico en el terminal o en la línea como el uso de receptores de barrido en los teléfonos móviles analógicos;

3) personas cercanas al terminal del receptor;

b) recordar al personal que no debería mantener conversaciones confidenciales en lugares públicos o en oficinas abiertas o salas de paredes delgadas;

c) no dejar mensajes en contestadores automáticos que puedan ser reproducidos por personas no autorizadas, grabarse en sistemas de uso público o grabarse incorrectamente como resultado de una equivocación en el marcado;

d) recordar al personal los problemas en el uso de máquinas fax, concretamente:

1) el acceso no autorizado a los almacenamientos internos de mensajes para recuperarlos;

2) la programación deliberada o accidental de las máquinas para enviar mensajes a números específicos;

3) el envío de documentos y mensajes a un número equivocado, procedente del marcado o recuperación desde el almacenamiento de números.

9. CONTROL DE ACCESOS

9.1 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.

9.1.1 Política de control de accesos

9.1.1.1 Política y requisitos de negocio

Deberían definirse y documentarse los requisitos del negocio para el control de accesos. Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. 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;

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);

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 capitulo 12);

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.

9.1.1.2 Reglas de los controles de accesos

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 5.2) 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.

9.2 Gestión de acceso de usuarios

OBJETIVO: Evitar 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 cielo 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.

9.2.1 Registro de usuarios

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.

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;

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 9.1) 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 inciso 8.1.4);

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;

j) la garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

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 también 6.1.4 y 6.1.5).

9.2.2 Gestión de privilegios

Debería restringirse y controlarse el uso y asignación de privilegios (cualquier prestación o recurso de un sistema de información multiusuario que permita evitar controles del sistema o de la aplicación). El uso inadecuado de privilegios en el sistema, muchas veces se revela

como el factor principal que contribuye al fallo de los sistemas que han sido atacados con éxito.

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", 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) Asignar los privilegios a un identificador de usuario distinto al asignado para un uso normal.

9.2.3 Gestión de contraseñas de usuario

Las contraseñas son medios, de uso corriente, para validar la identidad de un usuario con el fin de acceder a un sistema o servicio de información. Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal que debería:

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 6.1.4);

b) proporcionar inicialmente una contraseña temporal segura que forzosamente deben cambiar inmediatamente después. Se deberían proporcionar también contraseñas temporales cuando un usuario olvide la suya sólo tras una identificación positiva del usuario;

c) 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. Los usuarios deberían remitir acuse de recibo de sus contraseñas.

Nunca se deberían almacenar las contraseñas en un sistema informático sin protegerlas con otras tecnologías que las ya usadas para la identificación y autenticación de usuarios, por ejemplo, con las biométricas (como la verificación de huellas, la verificación de la firma) o el uso de dispositivos hardware (como las tarjetas inteligentes).

9.2.4 Revisión de los derechos de acceso de los usuarios

Para mantener un control efectivo del acceso a los datos y servicios de información, la gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. Este proceso debería:

a) revisar los derechos de acceso de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses) y después de cualquier cambio (véase el inciso 9.2.1);

b) revisar más frecuentemente (se recomienda cada tres meses) las autorizaciones de derechos de acceso con privilegios especiales (véase el inciso 9.2.2);

c) comprobar las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados.

9.3 Responsabilidades de los usuarios

OBJETIVO: Evitar el acceso de usuarios no autorizados.

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.

9.3.1 Uso de contraseñas

Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.
Las contraseñas ofrecen un medio de validar la identidad de cada usuario, pudiendo así establecer los derechos de acceso a los recursos o servicios de tratamiento de la información. Todos los usuarios deberían ser informados acerca de:

a) mantener la confidencialidad de las contraseñas;

b) evitar la escritura de las contraseñas en papel, salvo si existe una forma segura de guardarlo;

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 de 6 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) 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.

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.

9.3.2 Equipo informático de usuario desatendido

Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos. El equipo informático instalado en zonas de usuario por ejemplo, puestos de trabajo o servidores de archivos puede requerir protección específica contra accesos no autorizados cuando se dejan desatendidos un largo periodo de tiempo. 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.

9.4 Control de acceso a la red

OBJETIVO: Protección 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.

9.4.1 Política de uso de los servicios de la red

Las conexiones inseguras a los servicios de la red pueden afectar al conjunto de la organización. Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica. Este control es particularmente importante en conexiones a aplicaciones sensibles, críticas o por usuarios conectados desde lugares de alto riesgo, por ejemplo, en áreas públicas o situadas fuera de la gestión y los controles de seguridad de la organización.

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. Esta política debería ser coherente con la política de control de accesos de la organización (véase el inciso 9.1).

9.4.2 Ruta forzosa

La ruta de conexión desde el terminal del usuario hasta los servidores informáticos puede necesitar estar controlada. Las redes se diseñan con dispositivos para maximizar la compartición de recursos y la flexibilidad de rutas. Estos dispositivos también abren posibilidades de accesos no autorizados a las aplicaciones o de uso no autorizado de los recursos de información. Estos riesgos pueden reducirse mediante controles que restrinjan la ruta de acceso desde el terminal del usuario a los servidores informáticos, por ejemplo, el establecimiento de una ruta forzosa.

El objetivo de una ruta forzosa es impedir que un usuario seleccione otros caminos al margen de la ruta entre el terminal del usuario y los servidores a los que el usuario está autorizado a acceder.

Esto requiere implantar cierto número de medidas en distintos puntos de la ruta. El objeto es limitar las opciones de posibles rutas en cada punto de la red a elecciones predeterminas.

Ejemplos de rutas forzosas son:

a) utilizar líneas o números de teléfono dedicados;

b) conectar automáticamente puertos a sistemas de aplicaciones específicas o a gateways de seguridad;

c) limitar las opciones de menú para usuarios particulares;

d) evitar los recorridos cíclicos ilimitados en la red;

e) forzar el uso por usuarios de redes externas de ciertos sistemas de información específicos y/o gateways de seguridad;

f) controlar activamente las comunicaciones emitidas de origen a destino por medio de gateways de seguridad, por ejemplo, firewall;

g) restringir el acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para ciertos grupos de usuarios dentro de la organización (véase también el inciso 9.4.6).

Los requisitos para una ruta forzada se deberían basar en la política de control de accesos (véase el inciso 9.1).

9.4.3 Autenticación de usuarios para conexiones externas

Las conexiones externas son una fuente potencial de accesos no autorizados a la información, por ejemplo, las realizadas con sistemas de acceso por línea telefónica y módem. Por tanto, el acceso por usuarios remotos debería ser objeto de su autenticación. De los distintos métodos de autenticación, unos proporcionan más protección que otros, así los basados en técnicas de cifrado pueden dar una autenticación fuerte. Es importante determinar qué nivel de protección es requerido a partir de una evaluación de riesgos, lo que se necesita para seleccionar adecuadamente el método de autenticación.

La autenticación de los usuarios remotos puede lograrse, por ejemplo, usando una técnica criptográfica, mecanismos de hardware o protocolos adecuados. También pueden usarse líneas privadas dedicadas o un mecanismo de verificación de la dirección del usuario en la red para asegurarse del origen de las 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.

9.4.4 Autenticación de nodos de la red

Los dispositivos de conexión remota automática significan una amenaza de accesos no autorizados a las aplicaciones. Por tanto, se deberían autenticar las conexiones a sistemas informáticos remotos. Esto es muy importante si la conexión usa una red cuyo control escapa a la gestión de seguridad de la organización. En el inciso anterior 9.4.3 se han dado varios ejemplos de autenticación y cómo conseguirla.

La autenticación de nodos puede ser una alternativa a la autenticación de grupos de usuarios remotos, cuando éstos estén conectados a un sistema compartido seguro (véase el inciso 9.4.3).

9.4.5 Protección a puertos de diagnóstico remoto

Debería controlarse de una manera segura el acceso a los puertos de diagnóstico. En muchos computadores y sistemas de comunicación se instala un servicio de conexión dial-up para que los ingenieros de mantenimiento puedan realizar diagnósticos remotos. Estos puertos pueden permitir accesos no autorizados si no están protegidos. Por tanto, se deberían proteger con un mecanismo de seguridad adecuado, por ejemplo, un cierre y un procedimiento para asegurar que sólo son accesibles tras el acuerdo entre el director del servicio informático y el personal de mantenimiento del hardware o software que solicita acceso.

9.4.6 Segregación en las redes

Las redes se extienden cada día más allá de las fronteras tradicionales de las organizaciones, al establecerse asociaciones que requieren conexión o compartir recursos informáticos y prestaciones de redes. Estas extensiones pueden incrementar los riesgos de accesos no autorizados a los actuales sistemas de información conectados a las redes. Algunos de éstos albergan servicios y datos sensibles o críticos que pueden requerir protecciones adicionales frente a otros usuarios de la red. En tales circunstancias, se debería considerar la introducción de controles en la red para segregar grupos de servicios de información, usuarios y sistemas de información.

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. 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 9.4.7 y 9.4.8) y bloquee los accesos no autorizados de acuerdo con la política de control de accesos de la organización (véase el inciso 9.1). Un ejemplo de este tipo de gateway es lo que comúnmente se conoce como firewall.

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 9.1) 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 9.4.7 y 9.4.8).

9.4.7 Control de conexión a las redes

Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, necesitan incorporar controles que restrinjan las capacidades de conexión de los usuarios. Estos controles pueden establecerse mediante gateway que filtren el tráfico entre redes por medio de tablas o reglas predefinidas. Las restricciones que se impongan se deberían basar en los requisitos de las aplicaciones del negocio (véase el inciso 9.1) y se deberían mantener y actualizar de acuerdo a ellos. Estas restricciones podrían ser, por ejemplo:

a) correo electrónico;

b) transferencia de archivos en una sola dirección;

c) transferencias de archivos en ambas direcciones;

d) acceso interactivo;

e) acceso desde la red limitado a días de la semana u horas concretas.

9.4.8 Control de enrutamiento en la red

Las redes compartidas, especialmente las que cruzan las fronteras de la organización, pueden requerir 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 (véase el inciso 9.1). Este control suele ser esencial en redes compartidas con usuarios ajenos a la organización.

Los controles del enrutamiento podrían basarse en mecanismos positivos de verificación de las direcciones de origen y destino de los mensajes. La conversión de direcciones de la red también es un mecanismo muy útil para aislar redes y evitar rutas de propagación desde la red de una organización a la red de otra. Su implementación, mediante software o hardware, debería tener en cuenta la robustez de los propios mecanismos empleados.

9.4.9 Seguridad de los servicios de red

Está disponible un amplio rango de servicios de red públicos y privados, algunos de los cuales ofrecen servicios de valor añadido. Los servicios de red pueden tener características de seguridad únicas o complejas. Las organizaciones que usen estos servicios, deberían asegurarse que se entrega una descripción clara de los atributos de seguridad de todos los servicios utilizados.

9.5 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, y si procede, el terminal o la ubicación física del mismo;

b) registrar los accesos satisfactorios y fallidos al sistema;

c) suministrar mecanismos, adecuados de autenticación; si se utiliza un sistema de gestión de contraseñas, se debería asegurar la calidad de las mismas;

d) cuando proceda, restringir los tiempos de conexión de usuarios.

Otros métodos de control de acceso, tales como pregunta de reconocimiento-respuesta, están disponibles si están justificados en base al riesgo del negocio.

9.5.1 Identificación automática de terminales

Debería considerarse el uso de la identificación automática de terminales para autenticar las conexiones a ubicaciones específicas y a equipos portátiles. Esta técnica se usa si es importante que la sesión pueda establecerse sólo desde ubicaciones o terminales determinados. Se utiliza un identificador dentro del terminal o unido a él para indicar si desde él pueden iniciarse o recibirse transacciones determinadas. Se necesita también aplicar algún sistema de protección física al terminal para proteger la seguridad de su identificador. También pueden emplearse otras técnicas para la autenticación de usuarios (véase el inciso 9.4.3).

9.5.2 Procedimientos de conexión de terminales

El acceso a los servicios de información debería estar disponible mediante un proceso de conexión seguro. 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;

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.

9.5.3 Identificación y autenticación del usuario

Todos los usuarios (incluidos los administradores de red y de bases de datos, los programadores de sistemas y el personal técnico de apoyo) deberían disponer de un identificador único para su uso personal y exclusivo, a fin de que pueda posteriormente seguirse la pista de las actividades de cada responsable particular. Los identificadores no deberían dar indicación alguna del nivel de privilegio del usuario, por ejemplo, supervisor, director, etc. (véase el inciso 9.2.2).

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.

Distintos procedimientos de autenticación pueden usarse para materializar la identidad pedida a un usuario. Las contraseñas (véase también el inciso 9.3.1 y siguientes) 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.

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.

9.5.4 Sistema de gestión de contraseñas

Las contraseñas son uno de los medios básicos para validar la autorización a un usuario, para su acceso a los servicios informáticos. Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas (véase el inciso 9.3.1 como guía para el uso de contraseñas).

Algunas aplicaciones requieren que las contraseñas se asignen por una autoridad independiente. En la mayoría de los casos, los propios usuarios seleccionan y mantienen sus contraseñas.

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 como se describe en el inciso 9.3.1;

d) imponer el cambio de contraseñas como se describe en el inciso 9.3.1 si son los usuarios quienes las mantienen;

e) imponer el cambio de contraseñas iniciales en la primera conexión (véase el inciso 9.2.3) si son los usuarios quienes las escogen;

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;

j) después de instalar el software, cambiar las contraseñas que proporciona su proveedor por defecto.

9.5.5 Utilización de las facilidades del sistema

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. Los controles siguientes deberían ser considerados:

a) usar procedimientos de autenticación 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;

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 todas las facilidades basadas en software y el software de sistemas que no sean necesarios.

9.5.6 Protección del usuario frente a coacciones

Los usuarios que pueden ser objeto de una coacción deberían protegerse con mecanismos de disparo de alarma anti-coacción. La decisión de proveer este tipo de alarma debería basarse en una evaluación de riesgos. Se deberían definir procedimientos y responsabilidades para reaccionar ante una alarma anti-coacción.

9.5.7 Desconexión automática de terminales

Se deberían desactivar tras un periodo definido de inactividad los terminales situados en lugares de alto riesgo, en áreas públicas o no cubiertas por la gestión de seguridad de la organización, o que sirvan a sistemas de alto riesgo, para evitar el acceso de personas no autorizadas. 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 y de los usuarios del terminal.

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.

9.5.8 Limitación del tiempo de conexión

Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo. Limitar el periodo de tiempo durante el que se aceptan conexiones desde un terminal reduce la 'ventana' de oportunidad para accesos no autorizados. 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.

9.6 Control de acceso a las aplicaciones

OBJETIVO: Evitar 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;

d) proporcionar acceso a la información sólo a su propietario, a otras personas autorizadas nominalmente o a grupos de usuarios específicos.

9.6.1 Restricción de acceso a la información

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, basada en requisitos específicos de la aplicación y consistente con la política de acceso a la información de la organización (véase el inciso 9.1). Deberían considerarse las siguientes medidas y controles 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) restringir el conocimiento de información y de funciones del sistema de aplicaciones a cuyo acceso los usuarios no estén autorizados, editando adecuadamente la documentación de usuario;

c) controlar los derechos de acceso de los usuarios, por ejemplo lectura, escritura, borrado, ejecución;

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.

9.6.2 Aislamiento de sistemas sensibles

Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados). 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:

a) el propietario de la aplicación debería indicar explícitamente y documentar la 'sensibilidad' de ésta (véase el inciso 4.1.3);

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.

9.7 Seguimiento de accesos y usos del sistema

OBJETIVO: Detectar actividades no autorizadas.

Debería efectuarse un seguimiento y control de los sistemas para detectar desviaciones de la política de control de accesos y registrar los eventos observables que proporcionen evidencias en caso de incidencias de seguridad.

El seguimiento y control del sistema permite comprobar la efectividad de los controles instalados y verificar la conformidad con un modelo de política de accesos (véase el inciso 9.1).

9.7.1 Registro de incidencias

Deberían mantenerse durante un período adecuado registros de auditoría con las excepciones y otras incidencias importantes para la seguridad que permitan futuras investigaciones y el seguimiento del control de los accesos. Estos registros de auditoría deberían contener también:

a) el identificador del usuario;

b) fecha y hora de conexión y desconexión;

c) identificación del terminal o el lugar si es posible;

d) registro de los intentos aceptados y rechazados de acceso al sistema;

e) registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

Se tienen que archivar ciertos registros de auditoría como parte de la política de retención de registros o debido a requisitos para recojo de evidencias (véase también el capítulo 12).

9.7.2 Seguimiento del uso de los sistemas

9.7.2.1 Procedimientos y áreas de riesgo

Se necesitan procedimientos de seguimiento del uso de los recursos informáticos para asegurarse de que los usuarios únicamente realizan procesos para los que han sido autorizados de forma expresa. El nivel de seguimiento para los sistemas individualizados debería determinarse mediante un análisis de riesgos. Áreas que deberían ser consideradas incluyen:

a) el acceso autorizado, incluyendo detalles como:

1) el identificador de usuario;

2) fecha y hora de los eventos clave;

3) los tipos de eventos;

4) los archivos accedidos;

5) los programas o recursos usados;

b) todas las operaciones que requieren privilegios especiales, como:

1) uso de la cuenta del supervisor:

2) arranque y parada del sistema;

3) conexión o desconexión de un recurso de entrada o salida;

c) registro de los intentos aceptados y rechazados de acceso al sistema;

1) intentos fallidos;

2) violaciones de la política de accesos y notificaciones a los gateway y firewall;

3) alertas desde los sistemas de detección de intrusiones;

d) alertas o fallas del sistema, como:

1) alertas y mensajes de la consola;

2) excepciones al registro del sistema;

3) alarmas de gestión de la red.

9.7.2.2 Factores de riesgo

Se debería revisar regularmente el resultado de las actividades de seguimiento. La frecuencia de revisión debería depender de los riesgos implicados. Los factores de riesgo que deberían ser considerados incluyen:

a) la criticidad de los procesos de aplicación;

b) el valor, sensibilidad o criticidad de la información implicada;

c) la experiencia anterior sobre infiltración y mal uso del sistema;

d) la extensión de las interconexiones del sistema (en particular con redes públicas).

9.7.2.3 Incidencias de registro y revisión

La revisión de los registros implica la comprensión de las amenazas al sistema y la forma en que se presentan. En el inciso 9.7.1 se dan ejemplos de incidentes que deberían requerir más investigación si afectan a la seguridad.

Los registros del sistema suelen contener gran cantidad de información, en su mayor parte ajena al seguimiento de la seguridad. Para facilitar la identificación de eventos significativos con el propósito de seguimiento y control de la seguridad, debería considerarse la copia automática de los tipos de mensajes apropiados a un segundo registro y/o emplear los recursos convenientes del sistema o las herramientas de auditoría para realizar la revisión de los archivos.

Cuando se designen responsabilidades en la revisión de registros se debería realizar una segregación de funciones entre quienes realicen las actividades del seguimiento y quienes realicen su revisión.

Se debería poner especial atención a la seguridad del dispositivo de registro, porque si se manipula, conduce a una sensación falsa de seguridad. Se deberían tener en cuenta controles para protegerlo contra cambios no autorizados y problemas de funcionamiento como:

a) la desactivación del dispositivo de registro;

b) alteraciones del tipo de mensajes registrados;

c) la edición o borrado de archivos de registro;

d) la saturación de los medios de soporte del archivo de registro, no registrando eventos o grabando sobre otros registrados anteriormente.

9.7.3 Sincronización de relojes

La correcta sincronización de los relojes de los procesadores es esencial para la exactitud de los registros de auditoría que podría necesitar la investigación de incidencias o como prueba en casos legales o disciplinarios. La inexactitud de los registros de auditoría puede impedir las investigaciones y restar credibilidad a dicha evidencia.

Donde un computador o un dispositivo de comunicaciones pueda accionar un reloj de tiempo real, debería ajustarse a la norma acordada del Tiempo Universal Coordinado (UCT) o a la hora local normalizada acordada. Los relojes de procesador que puedan adelantarse o

retrasarse deberían requerir un procedimiento que compruebe y corrija las faltas de sincronizaciones importantes.

9.8 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.

9.8.1 Informática móvil

Se debería adoptar especial cuidado para asegurar que la información 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. Por ejemplo, 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 10.3), 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 inciso 8.3). Se debería disponer de equipos para realizar respaldos rápidos y fáciles de la información, a los que se debería dar la protección adecuada, por ejemplo, contra robo o pérdida.

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 9.4) 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. 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 7.2.5.

Se debería concientizar 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.

9.8.2 Teletrabajo

El teletrabajo usa tecnologías de comunicación para que el personal pueda trabajar de manera remota desde un lugar fijo situado fuera de su 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.

Las organizaciones deberían considerar el desarrollo de una política, procedimientos y normas para controlar las actividades de teletrabajo. Sólo deberían autorizarlas si se han satisfecho las disposiciones y controles de seguridad apropiados y se cumple la política de seguridad de la organización. 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.

Los controles y adecuaciones a ser consideradas incluyen:

a) el aprovisionamiento del equipo y mobiliario adecuados para las actividades de teletrabajo;

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) los procedimientos de respaldo y continuidad del negocio;

h) la auditoría y seguimiento de la seguridad;

i) la revocación de autorizaciones, derechos de acceso y devolución del equipo cuando cesen las actividades de teletrabajo.

10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

10.1 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, incluyendo las disposiciones para contingencias, 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.

10.1.1 Análisis y especificación de los requisitos de seguridad

Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control. Dichas 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 valoren paquetes de software para aplicaciones de negocio. Si es necesario, la gerencia puede optar por hacer uso de productos evaluados y certificados independientemente.

Los requisitos y controles de seguridad deberían reflejar el valor de los activos de información implicados y el posible daño a la organización que resultaría de fallos o ausencia de seguridad. La estimación del riesgo y su gestión son el marco de análisis de los requisitos de seguridad y de la identificación de los controles y medidas para conseguirla.
Los controles y medidas introducidos en la fase de diseño son mucho más baratos de implantar y mantener que los que se incluyen durante o tras la implantación.

10.2 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 y las pistas de auditoría o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Se pueden requerir medidas y controles adicionales en los sistemas que procesen o tengan impacto sobre activos sensibles, valiosos o críticos para la organización. Dichas medidas se deberían determinar a partir de los requisitos de seguridad y la estimación del riesgo.

10.2.1 Validación de los datos de entrada

Se deberían validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas. 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 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 autorizado 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;

10.2.2 Control del proceso interno

10.2.2.1 Áreas de riesgo

Los datos introducidos correctamente pueden corromperse por errores del proceso o por actos deliberados. Se deberían incorporar a los sistemas comprobaciones de validación para detectar dicha corrupción. El diseño de las aplicaciones debería asegurar la implantación de restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad. Áreas de riesgo específicas a considerar serían:

a) la ubicación y 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 inciso 8.1.1);

c) el uso de programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos.

10.2.2.2 Verificaciones y controles

Los controles requeridos dependerán de la naturaleza de la aplicación y del impacto de la corrupción de los datos en el negocio. 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 10.2.1);

d) comprobaciones de la integridad de los datos o del software transferidos desde o hacia el comprador central (véase el inciso 10.3.3);

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.

10.2.3 Autenticación de mensajes

La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados o una corrupción del contenido de un mensaje transmitido electrónicamente. Puede implantarse mediante hardware o software soportando un dispositivo físico de autenticación de mensajes o un algoritmo de software.

Se debería establecer la autenticación de mensajes en aplicaciones que requieran protección de la integridad del contenido de los mensajes, por ejemplo, transferencia electrónica de fondos, especificaciones, contratos, propuestas u otros intercambios electrónicos de datos importantes. Se pueden usar técnicas criptográficas (véanse los incisos 10.3.2 y 10.3.3) como un medio adecuado para implantar dicha autenticación.

La autenticación de mensajes no protege el contenido de la información frente a su divulgación no autorizada.

10.2.4 Validación de los datos de salida

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. Habitualmente la construcción de los sistemas parte de la premisa de su completa corrección si se han emprendido las adecuadas tareas de validación, verificación y prueba. Esto no es siempre cierto. 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.

10.3 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.

10.3.1 Política de uso de los controles criptográficos

La decisión sobre la idoneidad de una solución criptográfica debería verse como parte de un proceso más amplio de evaluación de riesgos y selección de medidas de control. Se debería realizar una evaluación de riesgos para determinar el nivel de protección que debería recibir la información. Evaluación que luego puede utilizarse para determinar si las medidas criptográficas son adecuadas, qué tipo de medida se debería aplicar, con qué propósito y en qué procesos del negocio.

La organización debería desarrollar una política de uso de las medidas criptográficas para proteger la información. Tal política es necesaria para maximizar los beneficios y minimizar los riesgos del uso de dichas técnicas, evitando su uso incorrecto o inapropiado. 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;

b) 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;
c) los papeles y responsabilidades de cada cual;

d) la implantación de la política;

e) la gestión de las claves;

f) la forma de determinar el nivel de protección criptográfico adecuado;

g) las normas a adoptar para su implantación eficaz a través de la organización (qué solución usar para qué procesos de negocio).

10.3.2 Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debería usar para la protección de información sensible o crítica.

El nivel adecuado de protección se debería basar en una evaluación del riesgo y tendrá en cuenta el tipo y calidad del algoritmo de cifrado y la longitud de las claves criptográficas que se usarán.

En la implantación de la política criptográfica de la organización se deberían tener en cuenta las regulaciones y restricciones nacionales que se aplican en distintas partes del mundo para el uso de las técnicas criptográficas y el cifrado de las transmisiones internacionales de datos. Además de los controles que se aplican a la exportación e importación de tecnología criptográfica (véase también el inciso 12.1.6).

Se debería contemplar el asesoramiento de especialistas para determinar el nivel apropiado de protección, para elegir los productos adecuados que proporcionen la protección requerida y la implantación de un sistema seguro de gestión de claves (véase también el inciso 10.3.5). Además se debería contemplar, la opinión de consultores legales sobre las leyes y regulación aplicables al uso previsto del cifrado en la organización.

10.3.3 Firmas digitales

Las firmas digitales proporcionan un medio de proteger 1a autenticidad y la integridad de los documentos electrónicos. Por ejemplo, se usan en el comercio electrónico cuando hay necesidad de verificar quién firma un documento electrónico y de verificar si el contenido del documento firmado ha sido cambiado.

Las firmas digitales pueden aplicarse a todo tipo de documento procesable electrónicamente, por ejemplo, para firmar pagos electrónicos, transferencias de fondos, contratos o acuerdos. Las firmas digitales pueden implantarse usando una técnica criptográfica basada en un único par de claves interrelacionadas, una para crear la firma (clave privada) y otra para comprobarla (clave pública).

Se debería cuidar la protección de la confidencialidad de la clave privada, que ha de mantenerse en secreto ya que todo el que acceda a ella puede firmar documentos como pagos o contratos como si 'falsificara' la firma del propietario de la clave. Asimismo, es importante la protección de la integridad de la clave pública, que se consigue usando un certificado de dicha clave pública (véase el inciso 10.3.5).

Se necesitan ciertas consideraciones sobre el tipo y calidad del algoritmo de firma y la longitud de la clave a utilizar. Las claves criptográficas usadas para las firmas digitales deberían ser distintas de las usadas para cifrado (véase el inciso 10.3.2).

Al usar las firmas digitales se debería tener en cuenta toda la legislación relativa que describe las condiciones en las que una firma digital tiene validez legal. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación legal de las firmas digitales. Puede haber necesidad de añadir contratos u otros acuerdos con validez legal para dar soporte al uso de las firmas digitales cuando el marco legal no sea adecuado. Se debería contemplar el asesoramiento legal sobre las leyes y regulación aplicables para el uso previsto de firmas digitales por la organización.

10.3.4 Servicios de no repudio

Se deberían utilizar servicios de no repudio cuando haya que resolver disputas sobre la ocurrencia o no de un evento o acción, por ejemplo, sobre el uso de una firma digital en un contrato o pago electrónico. Estos servicios ayudan a establecer la evidencia que constate si un evento o acción ha sucedido, por ejemplo, la denegación o envío por correo electrónico de una instrucción firmada digitalmente. Los servicios se basan en técnicas de cifrado y firmas digitales (véanse los incisos 10.3.2 y 10.3.3).

10.3.5 Gestión de claves

10.3.5.1 Protección de claves criptográficas

La gestión de las claves criptográficas es crucial para el uso eficaz de las técnicas criptográficas. Todo problema o pérdida de las claves criptográficas puede llevar a debilitar la autenticidad, confidencialidad y/o integridad de la información. Se debería instalar un sistema de gestión para dar soporte al uso por la organización de los dos tipos de técnicas criptográficas, que 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 (véase el inciso 10.3.2) y para producir firmas digitales (véase el inciso 10.3.3).

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.

10.3.5.2 Normas, procedimientos y métodos

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 auditorías 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.

Pueden ser necesarios procedimientos para atender las peticiones legales para acceder a las claves criptográficas, por ejemplo, cuando haya necesidad de la información cifrada en forma descifrada como prueba en una causa judicial.

Además de la gestión segura de las claves privadas y secretas, se debería requerir protección de las daves públicas contra la amenaza de falsificación de firma digital por alguien que reemplace la clave pública de un usuario por la suya. Este problema se resuelve usando certificados de clave pública. Estos certificados se deberían producir de forma que enlacen solamente con el propietario del par de claves pública y privada. Es importante que el proceso de gestión que genere esos certificados sea fiable. 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 4.2.2).

10.4 Seguridad de los archivos del sistema

OBJETIVO: Para asegurar que los proyectos de Tecnología de la Información (TI) y las actividades complementarias sean llevadas a cabo de una forma segura. El acceso a los archivos del sistema debería ser controlado.

El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezca las aplicaciones del sistema o el software.

10.4.1 Control del software en producción

Se debería controlar la implantación de software en los sistemas operativos. 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 responsable correspondiente autorización de la gerencia (véase el inciso 10.4.3).

b) Los sistemas operativos deberían tener sólo código ejecutable, si es posible.

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.

d) Se debería mantener un registro de auditoría de todas las actualizaciones a las librerías de programas en producción.

e) Se deberían retener las versiones anteriores de software como medida de precaución para contingencias.

El software adquirido que se use en sistemas operativos se debería mantener en el nivel de soporte del proveedor. Se debería adoptar toda decisión de mejora a nuevas versiones teniendo en cuenta la seguridad de la versión (por ejemplo la introducción de una nueva funcionalidad de seguridad que afecten a dicha versión). Se deberían aplicar parches al software cuando ayuden a eliminar o reducir las vulnerabilidades.

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.

10.4.2 Protección de los datos de prueba del sistema

Se deberían proteger y controlar los datos de prueba. Las pruebas de sistema y de aceptación, generalmente requieren un volumen de datos lo mas próximo posible al volumen real. 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 despersonalizar y anonimizar 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 auditoría.

10.4.3 Control de acceso a la librería de programas fuente

Para reducir la probabilidad de corrupción de los programas del sistema, se debería mantener un estricto control en el acceso a las librerías de programas fuente como los siguientes (véase también el inciso 8.3):

a) Si es posible, las librerías de programas fuentes no deberían residir en los sistemas operativos.

b) Se debería nombrar un encargado de la librería de programas para cada aplicación.

c) El personal de apoyo informático no debería tener libre acceso, sin restricción, a las librerías de programas fuentes.

d) Los programas en desarrollo o mantenimiento no se debería ubicar en librerías operativas de programas fuentes.

e) 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.

f) Los listados de programas se deberían mantener en un entorno seguro (véase el inciso 8.6.4).

g) Se debería mantener un registro de auditoría de todos los accesos a las librerías de programas fuentes.

h) Se deberían archivar las versiones anteriores de programas fuente, con indicación clara de las fechas y tiempos precisos de su periodo operativo, junto a todo el software de soporte, los controles de tareas, las definiciones de datos y los procedimientos.

i) El mantenimiento y copia de las librerías de programas fuente debería estar sujeta a procedimientos estrictos de control de cambios (véase el inciso 10.4.1).

10.5 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.

10.5.1 Procedimientos de control de cambios

Para minimizar la corrupción de los sistemas de información, se deberían mantener estrictos controles sobre la implantación de cambios. Se deberían exigir procedimientos formales de control de cambios que garanticen que la seguridad y los procedimientos de control no están debilitados, que los programadores de apoyo sólo tienen acceso a las partes del sistema que necesitan para su trabajo y que todo cambio proviene de un acuerdo y aprobación previos. Un cambio en el software de la aplicación puede causar impacto en el entorno operativo. La aplicación y sus procedimientos de control de cambios deberían estar integrados siempre que sea posible (véase también el inciso 8.1.2). 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 la forma de implantación que minimice la interrupción del negocio;

h) la garantía de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua;

i) el mantenimiento de un control de versiones de toda actualización del software;
j) el mantenimiento de un seguimiento de auditoría de todas las peticiones de cambio;

k) la garantía del cambio de la documentación operativa (véase el inciso 8.1.1) y de los procedimientos de usuario en función de la necesidad;

l) la garantía de la adecuación del tiempo de implantación de los cambios para no dificultar los procesos de negocio implicados.

Muchas organizaciones mantienen un entorno en el que los usuarios prueban el nuevo software y en el que separan los entornos de desarrollo y de producción. Esto permite controlar el nuevo software y aumentar la protección de la información operativa que se use para pruebas.

10.5.2 Revisión técnica de los cambios en el sistema operativo

Periódicamente es necesario efectuar cambios en el sistema operativo, por ejemplo, para instalar una nueva versión o un parche de software. 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. 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 11).

10.5.3 Restricciones en los cambios a los paquetes de software

No se recomiendan modificaciones a los paquetes de software. 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. Se deberían probar y documentar totalmente los cambios de forma que puedan volverse a aplicar a las actualizaciones del software si fuese necesario.

10.5.4 Canales encubiertos y código Troyano

Un canal encubierto puede comprometer la información por medios indirectos y ocultos. Estos canales secretos se pueden activar cambiando un parámetro accesible por los elementos seguros e inseguros del sistema informático o incrustando información en un flujo de datos. El código de tipo 'Troyano' se diseña precisamente para afectar a un sistema por medios no autorizados ni descubiertos a tiempo ni requeridos por el receptor o el usuario del programa. Los canales encubiertos y los códigos Troyanos raramente tienen lugar de forma accidental. En los lugares concernientes a canales encubiertos y códigos Troyanos, se debería considerar lo siguiente:

a) comprar programas solamente de fuente confiable;

b) comprar programas en código fuente de tal forma que el código pueda ser verificado;

c) usar productos evaluados;

d) inspeccionar todo código fuente antes de su uso operativo;

e) controlar el acceso y las modificaciones en todo código una vez instalado;

f) utilizar personal de confianza probada para trabajar en los sistemas clave.

10.5.5 Desarrollo externo del software

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 12.1.2);

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 del código;

f) pruebas antes de la implantación para detectar el código Troyano.

11. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

11.1 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 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.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad y pérdidas de servicio. Se deberían desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos. Planes que se deberían mantener y probar para que se integren con todos los demás procesos de gestión.

La gestión de la continuidad del negocio debería incluir controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales.

11.1.1 Proceso de gestión de la continuidad del negocio

Se debería instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio. Este 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;

b) 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;

c) considerar la adquisición de los seguros adecuados que formarán parte del proceso de continuidad del negocio;

d) formular y documentar una estrategia de continuidad del negocio consistente con los objetivos y las prioridades del negocio acordados;

e) formular y documentar planes de continuidad del negocio en línea con la estrategia acordada;

f) probar y actualizar regularmente los planes y procesos instalados;

g) 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, por ejemplo, al comité de seguridad de la información (véase el inciso 4.1.1).

11.1.2 Continuidad del negocio y análisis de impactos

El estudio para la continuidad del negocio debería empezar por la identificación de los 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 el impacto de dichas interrupciones (en términos tanto de escala de daños como de periodo de recuperación). La evaluación debería considerar todos los procesos del negocio sin limitarse a los dispositivos informáticos. Ambas actividades se deberían realizar implicando totalmente a los propietarios de los recursos y procesos del negocio.

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. La gerencia deberá respaldar dicho plan.

11.1.3 Redacción e implantación de planes de continuidad

Se deberían desarrollar planes de mantenimiento y recuperación en el plazo requerido de las operaciones del negocio, tras la interrupción o la falla de sus procesos críticos. 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 implantación de procedimientos de emergencia para la recuperación en los plazos requeridos, atendiendo en particular a la evaluación de las dependencias externas del negocio y los contratos vigentes;

c) 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.

11.1.4 Marco de planificación para la continuidad del negocio

Se debería mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes y para identificar las prioridades de prueba y mantenimiento. Cada plan de continuidad del negocio debería 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.

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 y/o vidas humanas. Esto debería incluir acuerdos sobre la gestión de las relaciones públicas y un enlace efectivo con las autoridades públicas apropiadas como la policía, los bomberos y el gobierno local;

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) los procedimientos de reanudación que describen las acciones a realizar para que las operaciones del negocio vuelvan a la normalidad;

e) un calendario de mantenimiento que especifique cómo y cuándo se harán pruebas del plan, así como el proceso para su mantenimiento;

f) actividades de concientización y formación diseñadas para comprender los procesos de continuidad del negocio y asegurar que los procesos prosigan con eficacia;

g) las responsabilidades de las personas, describiendo a cada responsable de la ejecución de cada etapa del plan. Si se requiere se debería nombrar suplentes.

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.

11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

11.1.5.1 Prueba de los planes

Los planes de continuidad del negocio pueden fallar en la prueba, debido con frecuencia a supuestos incorrectos, descuidos o cambios en el equipo o en el personal. Por tanto, se deberían probar regularmente para asegurarse de su actualización y eficacia. Estas pruebas, también deberían asegurar que todos los miembros del equipo de recuperación y otras personas a quien corresponde están al tanto de los planes.

El calendario de pruebas para plan(es) de continuidad del negocio deberían 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.

11.1.5.2 Mantenimiento y reevaluación de los planes

Los planes de continuidad del negocio se deberían mantener con ayuda de revisiones y actualizaciones regulares para asegurar características la continuidad de su eficacia (véanse los incisos 11.1.1 a 11.1.3). Se deberían incluir procedimientos en el programa de gestión de los cambios de la organización para asegurar que características de la continuidad del negocio se están dirigiendo de la manera apropiada.

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).

12. CUMPLIMIENTO

12.1 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).

12.1.1 Identificación de la legislación aplicable

Se deberían definir y documentar de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información. Así como los controles, medidas y responsabilidades específicos para su cumplimiento.

12.1.2 Derechos de propiedad intelectual (DPI)

12.1.2.1 Derechos de autor

Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales sobre el uso del material protegido por derechos de propiedad intelectual, como: derechos de autor, derechos de diseño o marcas registradas. El infringir el derecho de autor puede conducir a acciones legales que impliquen procedimientos judiciales.

Los requisitos legales, regulatorios y contractuales pueden plantear restricciones a la copia de material protegido. En particular pueden requerir que sólo pueda utilizarse material desarrollado por la organización o bien proporcionado por el proveedor y bajo su licencia para la organización.

12.1.2.2 Derechos de autor del software

Los productos de software propietario se suelen entregar con un contrato de licencia que limite el uso de los productos a máquinas especificadas y a la creación de copias de respaldo solamente. Se deberían considerar los controles siguientes:

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) publicar normas para los procedimientos de adquisición de productos de software;

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) 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 auditoría;

k) cumplir los términos y condiciones de uso del software y de la información obtenida de redes públicas (véase también el inciso 8.7.6).

12.1.3 Salvaguarda de los registros de la organización

Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación. 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.

Se suelen clasificar los registros por tipos: registros contables, registros de bases de datos, registros de transacciones, registros de auditoría 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 se deberían guardar de forma segura y sólo se entregarán a las personas autorizadas cuando las necesiten (véanse los incisos 10.3.2 y 10.3.3).

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.

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 de manera aceptable por un tribunal, por ejemplo, todos los registros requeridos se puedan recuperar en un tiempo y un formato aceptables.

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.

12.1.4 Protección de los datos y de la privacidad de la información personal

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). 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.

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. El responsable del tratamiento, debería informar al encargado de su protección, sobre toda intención de registrar información personal en un

archivo estructurado, así como la responsabilidad de concientizar sobre los principios de protección de datos que define la legislación correspondiente.

12.1.5 Evitar el mal uso de los recursos de tratamiento de la información

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. 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 apropiada.

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. Se debería pedir asesoría legal antes de la implantación de estos procedimientos de supervisión y control.

Muchos países ya tienen o van camino de establecer 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. Por tanto, es esencial que todos los usuarios sean conscientes del alcance preciso del acceso que se les permite. 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.

12.1.6 Regulación de los controles criptográficos

Algunos países han puesto en vigor acuerdos, leyes, reglamentos u otros instrumentos para controlar el acceso o uso de controles criptográficos. Este control puede incluir:

a) la importación y/o exportación de hardware y software para realizar funciones criptográficas;

b) la importación y/o exportación de hardware y software que incluya funciones criptográficas;

c) 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.

12.1.7 Recopilación de pruebas

12.1.7.1 Reglas para las pruebas

Es necesario tener pruebas adecuadas para apoyar una acción contra una persona u organización. Cuando esta acción sea materia disciplinaria interna, la prueba se debería describir dentro de los procedimientos internos.

Cuando la acción esté relacionada con la legislación, civil o penal, las pruebas presentadas deberían estar conformes con las reglas establecidas por la legislación aplicable o por el Tribunal que sigue el caso. En general estas reglas cubren:

a) la admisibilidad de la prueba: que pueda o no utilizarse ante un Tribunal;

b) el peso de la prueba: la calidad y totalidad;

c) la pertinencia de la prueba de que los controles han funcionado correcta y consistentemente (la prueba del control del proceso) durante el periodo de almacenamiento y proceso por el sistema de la prueba a recuperar.

12.1.7.2 Admisibilidad de las pruebas

Para conseguir la admisibilidad de una prueba, las organizaciones deberían asegurar que su sistema de información cumple cualquier norma o código de buenas prácticas publicado para producir pruebas admisibles.

12.1.7.3 Calidad y totalidad de las pruebas

Para conseguir la calidad y totalidad de una prueba se necesita un rastro convincente de ella. En general dicho rastro bien fundamentado podrá establecerse bajo las siguientes condiciones:

a) Para documentos en papel el original está guardado de forma segura y se registra quién, dónde, cuándo lo encontró y quién atestiguó el descubrimiento. Cualquier investigación debería asegurar que los originales no se manipularán.

b) Para información en un medio informático: para asegurar su disponibilidad se deberían hacer copias de todo medio removible, esté la información en disco duro o en memoria. Se debería guardar el registro de todas las acciones realizadas durante el

proceso de copia, del que se buscarán testigos y se debería mantener en lugar seguro una copia de los medios y el registro.

Cuando se detecte un incidente, al principio no es obvio que se convierta en una posible acción ante el juzgado. Sin embargo, existe el peligro de que las pruebas se destruyan accidentalmente antes de que se confirme la seriedad del incidente. Es aconsejable acudir pronto al juzgado o a la policía en toda acción legal que se contemple y pedir consejo sobre la prueba requerida.

12.2 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.

12.2.1 Conformidad con la política de seguridad

Los gerentes deberían asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Además, se deberían considerar todas las áreas de la organización para realizar revisiones regulares que aseguren el cumplimiento de las políticas y normas de seguridad, debiendo incluir las siguientes:

a) sistemas de información;

b) proveedores de sistemas;

c) propietarios de información y de activos de información;

d) usuarios;

e) la gestión.

Se deberían hacer revisiones regulares a los propietarios de sistemas de información (véase el inciso 5.1) sobre la conformidad en sus sistemas de las políticas, normas y cualquier otro requisito apropiado de seguridad. El seguimiento operativo del uso del sistema se cubre por el inciso 9.7.

12.2.2 Comprobación de la conformidad técnica

Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información. La comprobación de la conformidad técnico implica el examen de los sistemas operativos para asegurar que se han implementado correctamente las medidas y controles de hardware y software. Este tipo de comprobación de la conformidad requiere la asistencia técnica de especialistas. La debería realizar manualmente 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.

La comprobación de la conformidad también incluye, por ejemplo, pruebas de intrusión, realizables por expertos independientes especialmente contratados para dicho fin. Esto puede ser muy útil para detectar vulnerabilidades en el sistema y para comprobar la eficacia de las medidas para evitar el consiguiente acceso no autorizado. En caso de que la prueba de intrusión tenga éxito, se debería tener la precaución de llegar a un compromiso entre la seguridad del sistema y la explotación inadvertida de otras vulnerabilidades.

Toda comprobación de la conformidad técnica sólo se debería realizar o supervisar por personas competentes y autorizadas.

12.3 Consideraciones sobre la auditoría de sistemas

OBJETIVO: Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.

Se deberían establecer controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías del sistema. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría.

12.3.1 Controles de auditoría de sistemas

Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio. Se debería observar lo siguiente:

a) Deberían acordarse los requisitos de auditoría 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 auditoría.

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.

h) Todos los procedimientos, requisitos y responsabilidades deberían estar documentados.

12.3.2 Protección de las herramientas de auditoría de sistemas

Se deberían proteger los accesos a las herramientas de auditoría de sistemas, por ejemplo, software o archivos de datos, para evitar cualquier posible mal uso o daño. Dichas herramientas deberían 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.

13. ANTECEDENTES

13.1.	ISO/IEC 17799:2000	Information technology – Code of practice for information security management
13.2.	UNE-ISO/IEC 17799:2002	Tecnología de la información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.