Compendio

Seguridad de la Información

Segunda edición

Título: Compendio Seguridad de la Información – Segunda edición

Diseño y Diagramación: ICONTEC

ISBN Impreso: 978-958-8585-53-6

ISBN Electrónico: 978-958-8585-54-3

Impresión: Contacto Gráfico Ltda.

Agosto de 2015

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC

ESTE COMPENDIO ESTÁ COMPRENDIDO POR LAS SIGUIENTES NORMAS:

NTC-ISO-IEC 27001
TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS.

GTC-ISO-IEC 27002
TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

GTC-ISO-IEC 27035
TECNOLOGÍA DE LA INFORMACIÓN. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001

2013-12-11

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS

E: INFORMATION TECHNOLOGY. SECURITY TECHNIQUES. INFORMATION SECURITY MANAGEMENT SYSTEMS. REQUIREMENTS.

CORRESPONDENCIA:	esta norma es una adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001: 2013.
DESCRIPTORES:	sistemas de gestión - seguridad de la información; información, técnicas de seguridad, gestión.

I.C.S.: 35.040

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

Primera actualización
Editada 2013-12-20

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La norma NTC-ISO-IEC 27001 (Primera actualización) fue ratificada por el Consejo Directivo de 2013-12-11.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 181 Gestión de la tecnología de la información.

AVIANCA S.A.
AZTECA COMUNUCACIONES
BANCO AGRARIO DE COLOMBIA S.A.
CENET S.A.
CROSS BORDER TECHNOLOGY S.A.S.
ECOPETROL - SLB
ESICENTER - SINERTIC
GEOCONSULT - ECP
HALLIBURTON - ECOPETROL
HELM BANK
INFOTRACK S.A.
INLAC
LA POLAR- CF
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
NEWNET S.A.
PROJECT ADVANCED MANAGEMENT
QUALITIC LTDA
SERVIENTREGA
TOP FACTORY

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

A TODA HORA S.A ATH
ACH COLOMBIA S.A.
ACTUALIZACIONES DE SISTEMAS LTDA.
AGENDA DE CONECTIVIDAD
ALFAPEOPLE ANDINO S.A.
ALIANZA SINERTIC
BANCO CAJA SOCIAL
BANCO COMERCIAL AV VILLAS
BANCO DAVIVIENDA S.A.
BANCO DE BOGOTÁ
BANCO DE LA REPÚBLICA
BANCO DE OCCIDENTE
BRANCH OF MICROSOFT COLOMBIA INC
CAJA COLOMBIANA DE SUBSIDIO FAMILIAR COLSUBSIDIO
CENTRO DE INVESTIGACIÓN Y DESARROLLO EN TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
CENTRO POLICLÍNICO DEL OLAYA C.P.O. S.A.
CHOUCAIR TESTING S.A.
CIBERCALL S.A.

COLOMBIA TELECOMUNICACIONES S.A. E.S.P.
COMERCIO ELECTRÓNICO EN INTERNET CENET S.A.
COMPUREDES S.A.
CONTRALORÍA DE CUNDINAMARCA
COOPERATIVA DE PROFESIONALES DE LA SALUD -PROSALCO I.P.S.-
CORREDOR EMPRESARIAL
CREDIBANCO
CRUZ ROJA COLOMBIANA SECCIONAL CUNDINAMARCA Y BOGOTÁ
DAKYA LTDA.
DIGIWARE
ECOPETROL S.A.
ENLACE OPERATIVO S.A.
ESCUELA COLOMBIANA DE CARRERAS INDUSTRIALES
ETB S.A. E.S.P.
FLUIDSIGNAL GROUP S.A.
FONDO DE EMPLEADOS DEL DEPARTAMENTO DE ANTIOQUIA
FUNDACIÓN PARQUE TECNOLÓGICO DEL SOFTWARE DE CALI -PARQUESOFT-
FUNDACIÓN UNIVERSITARIA INPAHU
GEMAS INGENIERIA Y CUNSULTORIA SAS
GESTIÓN & ESTRATEGIA S.A.S.
GETRONICS COLOMBIA LTDA.
GIT LTDA.
HMT S.A.S.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
INFOCOMUNICACIONES S.A.S.
INSTITUTO DE ORTOPEDIA INFANTIL ROOSEVELT
IPX LTDA.
IQ CONSULTORES
IT SERVICE LTDA.
JAIME TORRES C. Y CÍA. S.A.
JIMMY EXENOVER ESPINOSA LÓPEZ
KEXTAS LTDA.
LOGIN LEE LTDA.
MAKRO SUPERMAYORISTA S.A.
MAREIGUA LTDA.
MEGABANCO
MICROCOM COMUNICACIÓN Y SEGURIDAD LTDA.
NEGOTEC NEGOCIOS Y TECNOLOGÍA LTDA.
NEXOS SOFTWARE S.A.S.
PARQUES Y FUNERARIAS S.A. JARDINES DEL RECUERDO
PIRAMIDE ADMINISTRACION DE INFORMACION LTDA.
POLITÉCNICO MAYOR AGENCIA CRISTIANA DE SERVICIO Y EDUCACIÓN LTDA.
PONTIFICIA UNIVERSIDAD JAVERIANA
QUALITY SYSTEMS LTDA.
SISTEMAS Y FORMACIÓN S.A.S.
SOCIEDAD COLOMBIANA DE ARCHIVISTAS
SUN GEMINI S.A.
SYNAPSIS COLOMBIA LTDA.
TEAM FOODS COLOMBIA S.A.
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE COLOMBIA LTDA.
TELMEX COLOMBIA S.A.
TIQAL S.A.S
TOMÁS MORENO CRUZ Y CÍA. LTDA.
TRANSFIRIENDO S.A.
TRANSPORTADORA DE VALORES ATLAS LTDA.
TUS COMPETENCIAS LTDA.
UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNIVERSIDAD NACIONAL DE COLOMBIA
UNIVERSIDAD SANTIAGO DE CALI

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

Página

INTRODUCCIÓN i

0.1 GENERALIDADES i

0.2 COMPATIBILIDAD CON OTRAS NORMAS DE SISTEMAS DE GESTIÓN i

1. OBJETO Y CAMPO DE APLICACIÓN 1

2. REFERENCIAS NORMATIVAS 1

3. TÉRMINOS Y DEFINICIONES 1

4. CONTEXTO DE LA ORGANIZACIÓN 1

4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO 1

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS 2

4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2

4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2

5. LIDERAZGO 2

5.1 LIDERAZGO Y COMPROMISO 2

5.2 POLÍTICA 3

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN 3

6. PLANIFICACIÓN 4

6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES 4

Página

6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS 6

7. SOPORTE 6

7.1 RECURSOS 6

7.2 COMPETENCIA 6

7.3 TOMA DE CONCIENCIA 7

7.4 COMUNICACIÓN 7

7.5 INFORMACIÓN DOCUMENTADA 7

8. OPERACIÓN 8

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL 8

8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN 9

8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN 9

9. EVALUACIÓN DEL DESEMPEÑO 9

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN 9

9.2 AUDITORÍA INTERNA 10

9.3 REVISIÓN POR LA DIRECCIÓN 10

10. MEJORA 11

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS 11

10.2 MEJORA CONTINUA 12

DOCUMENTO DE REFERENCIA 26

Página

BIBLIOGRAFÍA **25**

ANEXO A (Normativo)
OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA **13**

INTRODUCCIÓN

0.1 GENERALIDADES

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.

La presente Norma puede ser usada por partes internas y externas para evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la propia organización.

El orden en que se presentan los requisitos en esta Norma no refleja su importancia ni el orden en el que se van a implementar. Los elementos de la lista se enumeran solamente para propósitos de referencia.

La ISO/IEC 27000 describe la visión general y el vocabulario de sistemas de gestión de la seguridad de la información, y referencia la familia de normas de sistemas de gestión de la seguridad de la información (incluidas las NTC-SO/IEC 27003[2], ISO/IEC 27004[3] y ISO/IEC 27005[4]), con los términos y definiciones relacionadas.

0.2 COMPATIBILIDAD CON OTRAS NORMAS DE SISTEMAS DE GESTIÓN

Esta Norma aplica la estructura de alto nivel, títulos idénticos de numerales, texto idéntico, términos comunes y definiciones esenciales definidas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado, y por tanto, mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que decidan poner en funcionamiento un único sistema de gestión que cumpla los requisitos de dos o más normas de sistemas de gestión.

TECNOLOGÍA DE LA INFORMACIÓN.
TÉCNICAS DE SEGURIDAD.
SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
REQUISITOS

1. OBJETO Y CAMPO DE APLICACIÓN

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Cuando una organización declara conformidad con esta Norma, no es aceptable excluir cualquiera de los requisitos especificados de los numerales 4 al 10.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

ISO/IEC 27000, *Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.*

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.3 de la NTC-ISO 31000:2011[5].

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La organización debe determinar:

a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y

b) los requisitos de estas partes interesadas pertinentes a seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.

4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el numeral 4.1, y

b) los requisitos referidos en el numeral 4.2; y

c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;

d) comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;

e) asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos;

f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) promoviendo la mejora continua, y

h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

5.2 POLÍTICA

La alta dirección debe establecer una política de la seguridad de la información que:

a) sea adecuada al propósito de la organización;

b) incluya objetivos de seguridad de la información (véase el numeral 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información;

c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; y

d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de la seguridad de la información debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización; y

g) estar disponible para las partes interesadas, según sea apropiado.

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;

b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.

6. PLANIFICACIÓN

6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

6.1.1 Generalidades

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones referidas en el numeral 4.1 y los requisitos a que se hace referencia en el numeral 4.2, y determinar los riesgos y oportunidades que es necesario tratar, con el fin de:

a) asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

   1) integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información,

   2) evaluar la eficacia de estas acciones.

6.1.2 Valoración de riesgos de la seguridad de la información

La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que:

a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan:

   1) Los criterios de aceptación de riesgos; y

   2) los criterios para realizar valoraciones de riesgos de la seguridad de la información;

b) asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identifique los riesgos de la seguridad de la información:

   1) aplicar el proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e

   2) identificar a los dueños de los riesgos;

d) analice los riesgos de la seguridad de la información:

1) Valorar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 c) 1);

2) Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 c) 1); y

3) determinar los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a) y

2) priorizar los riesgos analizados para el tratamiento de riesgos.

La organización debe conservar información documentada acerca del proceso de valoración de riesgos de la seguridad de la información.

6.1.3 Tratamiento de riesgos de la seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:

a) seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información;

NOTA Las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.

c) comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se han omitidos controles necesarios;

NOTA 1 El Anexo A contiene una lista amplia de objetivos de control y controles. Se invita a los usuarios de esta Norma a consultar el Anexo A, para asegurar que no se pasen por alto los controles necesarios.

NOTA 2 Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A;

e) formular un plan de tratamiento de riesgos de la seguridad de la información; y

f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.

La organización debe conservar información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.

NOTA El proceso de valoración y tratamiento de riesgos de la seguridad de la información que se presenta en esta Norma se alinea con los principios y directrices genéricas suministradas en la ISO 31000[5].

6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) ser coherentes con la política de seguridad de la información;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la valoración y del tratamiento de los riesgos;

d) ser comunicados; y

e) ser actualizados, según sea apropiado.

La organización debe conservar información documentada sobre los objetivos de la seguridad de la información.

Cuando se hace la planificación para lograr sus objetivos de la seguridad de la información, la organización debe determinar:

f) lo que se va a hacer;

g) que recursos se requerirán;

h) quién será responsable;

i) cuándo se finalizará; y

j) cómo se evaluarán los resultados.

7. SOPORTE

7.1 RECURSOS

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

7.2 COMPETENCIA

La organización debe:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y

b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3 TOMA DE CONCIENCIA

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de:

a) la política de la seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y

c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.

7.4 COMUNICACIÓN

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar; y

e) los procesos para llevar a cabo la comunicación.

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 Generalidades

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) la información documentada requerida por esta Norma; y

b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,

b) la complejidad de los procesos y sus interacciones, y

c) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta Norma se debe controlar para asegurarse de que:

a) esté disponible y adecuada para su uso, donde y cuando se necesite; y

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluida la preservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión); y

f) retención y disposición.

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar y controlar, según sea adecuado.

NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2.

La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario.

La organización debe asegurar que los procesos contratados externamente estén controlados.

8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a).

La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.

8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles.

c) cuándo se deben llevar a cabo el seguimiento y la medición;

d) quién debe llevar a cabo el seguimiento y la medición;

e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y

f) quién debe analizar y evaluar estos resultados.

La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

9.2 AUDITORÍA INTERNA

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) es conforme con:

   1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y

   2) los requisitos de esta Norma;

b) está implementado y mantenido eficazmente.

La organización debe:

c) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

d) para cada auditoría, definir los criterios y el alcance de ésta;

e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y

g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

NOTA Para mayor información consultar las normas NTC-ISO 19011 y NTC-ISO 27007

9.3 REVISIÓN POR LA DIRECCIÓN

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

La revisión por la dirección debe incluir consideraciones sobre:

a) el estado de las acciones con relación a las revisiones previas por la dirección;

b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;

c) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a:

   1) no conformidades y acciones correctivas;

   2) seguimiento y resultados de las mediciones;

3) resultados de la auditoría; y

4) cumplimiento de los objetivos de la seguridad de la información;

d) retroalimentación de las partes interesadas;

e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y

f) las oportunidades de mejora continúa.

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

10. MEJORA

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar ante la no conformidad, y según sea aplicable

1) tomar acciones para controlarla y corregirla, y

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

1) la revisión de la no conformidad

2) la determinación de las causas de la no conformidad, y

3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas, y

e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada adecuada, como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y

g) los resultados de cualquier acción correctiva.

10.2 MEJORA CONTINUA

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.

ANEXO A
(Normativo)

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Los objetivos de control y controles enumerados en la Tabla A.1 se obtienen directamente de la ISO/IEC 27002:2013[1], numerales 5 a 18 y están alineados con ella, y se deben usar en contexto con el numeral 6.1.3.

Tabla A.1. Objetivos de control y controles

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Continúa…

Tabla A.1. (Continuación)

A.6.2.2	Teletrabajo	*Control* Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	**Antes de asumir el empleo**	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación y cambio de empleo**	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Tabla A.1. (Continuación)

A.8	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsabilidad por los activos**	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3	**Manejo de medios**	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	*Control* Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Tabla A.1. (Continuación)

A.9	**CONTROL DE ACCESO**	
A.9.1	**Requisitos del negocio para control de acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	**Gestión de acceso de usuarios**	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Tabla A.1. (Continuación)

A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas.
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Tabla A.1. (Continuación)

A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Tabla A.1. (Continuación)

A.12.1.3	Gestión de capacidad	*Control* Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3 Copias de respaldo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4 Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5 Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Tabla A.1. (Continuación)

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
A.12.7.1	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Tabla A.1. (Continuación)

A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

Tabla A.1. (Continuación)

A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15 RELACIONES CON LOS PROVEEDORES		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2 Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Tabla A.1. (Continuación)

A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Tabla A.1. (Continuación)

A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* *Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización*
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

BIBLIOGRAFÍA

[1] ISO/IEC 27002:2013, *Information Technology. Security Techniques. Code of Practice for Information Security Controls.*

[2] GTC-ISO/IEC 27003:2012, Tecnología de la información. técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información.

[3] ISO/IEC 27004:2009, *Information Technology. Security Techniques. Information Security Management. Measurement.*

[4] ISO/IEC 27005:2011, *Information Technology. Security Techniques. Information Security Risk Management.*

[5] NTC-ISO 31000:2011, Gestión del riesgo. Principios y directrices.

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement. Procedures Specific to ISO*, 2012.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva*: ISO, 2013, 23 p. (ISO/IEC 27001:2013 (E)).

CROSS BORDER TECHNOLOGY

Productos y servicios especializados de consultoría en Seguridad de la información, Seguridad informática y Continuidad del negocio.

Servicios

- ISO 27001 – Implementación SGSI
- Outsourcing en seguridad de la información y continuidad
- Cumplimiento PCI DSS, ISAE 3402, SOX, Circulares Superintendencia Financiera
- Auditorías y análisis de riesgos
- Planes de continuidad y recuperación ante desastres BCP & DRP
- Pruebas de vulnerabilidad y hacking ético
- Análisis de cómputo forense
- Programas de sensibilización en seguridad de la información, basados en técnicas de Coaching y PNL

Productos

- **CSR 360:** Solución diseñada para apoyar la toma de decisiones, mediante la gestión centralizada de Continuidad, Seguridad y Riesgos de las Organizaciones.
- **CypherCage:** Solución para el intercambio seguro y automatizado de información sensible.
- **Distribuidores autorizados:**
  - **Datalocker:** Discos, USBs y DVDs cifrados por hardware (AES 256).
  - **Voom:** Equipos de copiado y análisis de cómputo forense.
  - **LucidPORT:** Solución para el ciframiento de información utilizando doble factor de autenticación.
  - **Fortinet:** Soluciones de seguridad entre las cuales se destacan: UTM, Firewall, VPNs, control de navegación, IPS.

www.crossbordertech.com
PBX: +57(1) 612–6688
Avenida (Carrera) 19 No. 118–95, Oficina 309
Bogotá, Colombia

Es una solución diseñada para apoyar la toma de decisiones, mediante la gestión centralizada de Continuidad, Seguridad y Riesgos de las Organizaciones.

Principales Características:

- ✓ **Adaptación:** La gestión de CSR se basa en la parametrización de los procesos propios y la cadena de valor de cada Organización.
- ✓ **Integración:** Gestión centralizada de diferentes sistemas de administración de riesgos (SGSI, Riesgo Operativo, Continuidad, entre otros).
- ✓ **Flexibilidad:** La solución permite la parametrización de todos sus módulos y un modelo de reportes que facilita hacer análisis y trazabilidad.
- ✓ **Cumplimiento:** Apoya el cumplimiento de **ISO 27001**, ISO 22301, ISO 31000, GEL (Gobierno en Línea), ISAE 3402, PCI DSS.
- ✓ **Acceso:** Conexión vía web y un completo esquema de manejo de usuarios, de acuerdo con los perfiles que intervienen en la gestión "CSR" de la Organización.

Funcionalidades / Módulos:

- ✓ Gestión de Activos y clasificación de información
- ✓ Gestión de Riesgos
- ✓ Continuidad de negocio
- ✓ Gestión de eventos e incidentes
- ✓ Indicadores y Reportes
- ✓ Mejora continua
- ✓ Cumplimiento
- ✓ Parámetros

GUÍA TÉCNICA COLOMBIANA GTC-ISO/IEC 27002

2015-07-22

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

E: INFORMATION TECHNOLOGY. SECURITY TECHNIQUES-CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

CORRESPONDENCIA:	esta norma es idéntica por traducción (IDT) de la norma ISO/IEC 27002:2013 + Technical Corrigendum 1: 2014
DESCRIPTORES:	seguridad de la información, controles de seguridad, tecnologías de la información, gestión de la seguridad, sistemas de gestión.

I.C.S.: 35.040

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

Editada 2015-07-29

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La guía GTC-ISO/IEC 27002 fue ratificada por el Consejo Directivo de 2015-07-22.

Esta guía está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta guía a través de su participación en el Comité Técnico 181 Gestión de la tecnología de la información.

ALFREDO LÓPEZ Y CÍA. LTDA.
ARCHIVO GENERAL DE LA NACIÓN
AUDIT TRUST SERVICES S.A.S.
AVIANCA
AZTECA COMUNICACIONES
BANCO AGRARIO DE COLOMBIA
BANCO DE OCCIDENTE
BANCO GNB SUDAMERIS
CENET S.A.
COMPENSAR
CROSS BORDER TECHNOLOGY
ETB
ÉTICA Y TECNOLOGÍA
FLUIDSIGNAL GROUP S.A.
GEMAS S.A.
GEOCONSULT CS LTDA.
GESTION & ESTRATEGIA S.A.S.
GOVERNATI
HALLIBURTON LATINOAMÉRICA
HELM BANK COLOMBIA
IDENTIAN S.A.S.
INSTITUTO COLOMBIANO DEL PETRÓLEO -ICP ECOPETROL-
ITEAM
LA POLAR -CF-
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES -MINTIC-
NET READY SOLUTIONS
NEWNET S.A.
ONAC
PACIFIC RUBIALES
PROJECT ADVANCED MANAGEMENTE
QUALTIC S.A.S.
SCHLUMBERGER
SERVIENTREGA
SOCIETAL SECURITY
THOMAS GREG & SONS
TOP FACTORY S.A.

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

A TODA HORA S.A.
ACDECC
ALIANZA SINERTIC
ASIBANCARIA
ATLAS TRANSVALORES
BANCO DE BOGOTÁ

BANCO DE LA REPÚBLICA
BUSINESS PROCESS SERVICES - BP SERVICES S.A.S.
CCIT
CHOUCAIR TESTING
CINTEL
COLSUBSIDIO
CORREDOR EMPRESARIAL S.A.
DAKYA
DIJIN
E.T.B
ECOPETROL
INGENIERIA SUSTENTABLE
IPX LTDA.
IQ INFORMATION QUALITY
IQ OUTSOURCING
JTCCIA
MAREIGUA
MEGABANCO
MUSSI
PIRAMIDE ADMINISTRACIÓN DE INFORMACIÓN LTDA.
PONTIFICIA UNIVERSIDAD JAVERIANA
SGS COLOMBIA
SOCEH
SOCIEDAD COLOMBIANA DE ARCHIVISTAS
SUN GEMINI S.A.
SYNAPSIS
TELEFONICA TELECOM
TELMEX
TMC & CÍA.
UNIVERSIDAD AUTÓNOMA OCCIDENTE
UNIVERSIDAD JAVERIANA
UNIVERSIDAD NACIONAL DE COLOMBIA
UNIVERSIDAD SANTO TOMAS
VISA

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

PRÓLOGO

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de los comités técnicos establecidos por la organización respectiva para tratar campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de mutuo interés. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de Tecnología de la Información, ISO e IEC han establecido EL comité técnico conjunto ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La ISO/IEC 27002 fue preparada por el comité técnico conjunto ISO/IEC JTC 1, Tecnologías de la Información, subcomité SC 27, Técnicas de Seguridad de T.I.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La segunda edición de la norma ISO/IEC 27002 cancela y reemplaza la primera edición (ISO/IEC 27002:2005), la cual ha sido revisada y estructurada técnicamente.

NOTA NACIONAL Esta edición cancela y reemplaza la norma NTC-ISO/IEC 27002:2007, la cual ha sido revisada y estructurada técnicamente.

CONTENIDO

Página

0. INTRODUCCIÓN i

0.1 ANTECEDENTES Y CONTEXTO i

0.2 REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN ii

0.3 SELECCIÓN DE CONTROLES ii

0.4 DESARROLLO DE SUS PROPIAS DIRECTRICES iii

0.5 CONSIDERACIONES SOBRE EL CICLO DE VIDA iii

0.6 NORMAS RELACIONADAS iii

1. OBJETO Y CAMPO DE APLICACIÓN 1

2. REFERENCIAS NORMATIVAS 1

3. TÉRMINOS Y DEFINICIONES 1

4. ESTRUCTURA DE ESTA GUÍA 1

4.1 NUMERALES 2

4.2 CATEGORÍAS DE CONTROL 2

5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN 2

5.1 DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN 2

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 5

6.1 ORGANIZACIÓN INTERNA 5

6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO 8

Página

7. SEGURIDAD DEL RECURSO HUMANO 11
7.1 ANTES DE ASUMIR EL EMPLEO 11
7.2 DURANTE LA EJECUCIÓN DEL EMPLEO 13
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO 16

8. GESTIÓN DE ACTIVOS 17
8.1 RESPONSABILIDAD POR LOS ACTIVOS 17
8.2 CLASIFICACIÓN DE LA INFORMACIÓN 19
8.3 MANEJO DE MEDIOS 22

9. CONTROL DE ACCESO 24
9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO 24
9.2 GESTIÓN DE ACCESO DE USUARIOS 27
9.3 RESPONSABILIDADES DE LOS USUARIOS 32
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 33

10. CRIPTOGRAFÍA 37
10.1 CONTROLES CRIPTOGRÁFICOS 37

11. SEGURIDAD FÍSICA Y DEL ENTORNO 40
11.1 ÁREAS SEGURAS 40
11.2 EQUIPOS 44

12. SEGURIDAD DE LAS OPERACIONES 51
12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES 51
12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS 54

Página

12.3 COPIAS DE RESPALDO....56

12.4 REGISTRO (*LOOGING*) Y SEGUIMIENTO....57

12.5 CONTROL DE SOFTWARE OPERACIONAL (*Control of Operational Software*)....60

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA....61

12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN....64

13. SEGURIDAD DE LAS COMUNICACIONES....65

13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES....65

13.2 TRANSFERENCIA DE INFORMACIÓN....67

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS....71

14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN....71

14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE....75

14.3 DATOS DE PRUEBA....82

15. RELACIONES CON LOS PROVEEDORES....83

15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES....83

15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES....87

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....89

16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN....89

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO....95

Página

17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN 95

17.2 REDUNDANCIAS 97

18. CUMPLIMIENTO 98

18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES 98

18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 102

BIBLIOGRAFÍA 105

DOCUMENTO DE REFERENCIA 107

0. INTRODUCCIÓN

0.1 ANTECEDENTES Y CONTEXTO

La presente guía está diseñada para uso por parte de las organizaciones, como referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) con base en la NTC-ISO/IEC 27001[10], o como un documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Esta guía está prevista para uso en el desarrollo de directrices de gestión de la seguridad de la información específicas para la industria y las organizaciones, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información

Las organizaciones de cualquier tipo y tamaño (incluido el sector público y privado, comercial y sin ánimo de lucro) recolectan, procesan, almacenan y transmiten información en muchas formas, que incluyen los formatos electrónico, físico y las comunicaciones verbales (por ejemplo, conversaciones y presentaciones).

El valor de la información va más allá de las palabras escritas, números e imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas de información intangibles. En un mundo interconectado, la información y los procesos relacionados, los sistemas, las redes y el personal involucrado en su operación, el manejo y la protección de los activos que, como cualquier otro activo importante del negocio, son valiosos para el negocio de una organización, y en consecuencia ameritan o requieren protección contra diversos peligros.

Los activos son objeto de amenazas tanto deliberadas como accidentales, mientras que los procesos, sistemas, redes y personas relacionadas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas del negocio u otros cambios externos (como nuevas leyes y reglamentos) pueden crear nuevos riesgos de seguridad de la información. Por tanto, dada la multitud de formas en las que las amenazas pueden aprovecharse de las vulnerabilidades para perjudicar la organización, siempre hay presencia de riesgos de seguridad de la información. Una seguridad de la información eficaz reduce estos riesgos protegiendo a la organización contra amenazas y vulnerabilidades, y en consecuencia reduce los impactos en sus activos.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizacionales y las funciones del software y del hardware. Es necesario establecer, implementar, hacer seguimiento, revisar y mejorar estos controles en donde sea necesario, para asegurar que se cumplen los objetivos del negocio y de seguridad específicos de la organización. Un SGSI como el que se especifica en la norma NTC-ISO/IEC 27001[10] asume una visión holística y coordinada de los riesgos de seguridad de la información para implementar un conjunto amplio de controles de seguridad de la información bajo el marco de referencia global de un sistema de gestión coherente.

Muchos sistemas de información no han sido diseñados para ser seguros, en el sentido de la NTC-ISO/IEC 27001[10] y de esta guía. La seguridad que se puede lograr por medios técnicos es limitada y debería estar apoyada en gestión y procedimientos apropiados. La identificación

de los controles con los que se debería contar requiere una planificación cuidadosa y atención a los detalles. Un SGSI exitoso requiere el apoyo de todos los empleados de la organización. También requiere la participación de los accionistas, proveedores u otras partes externas. También puede ser necesaria asesoría especializada de las partes externas.

En un sentido más general, una seguridad de la información eficaz también asegura a la dirección y a otras partes interesadas, que los activos de la organización están razonablemente seguros y protegidos contra daño, y de esta manera actúa como un facilitador del negocio.

0.2 REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

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

a) la valoración de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos de negocio globales de la organización. Por medio de una valoración de riesgos se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la posibilidad de que ocurran, y se estima el impacto potencial;

b) los requisitos legales, estatutarios, de reglamentación y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios deben cumplir, y su entorno socio-cultural.

c) el conjunto de principios, objetivos y requisitos del negocio para el manejo, procesamiento, almacenamiento, comunicación y archivo de información, que una organización ha desarrollado para apoyar sus operaciones.

Es necesario establecer un balance entre los recursos empleados en la implementación de controles, y el daño para el negocio que pudiera resultar de cuestiones de seguridad en ausencia de tales controles. Los resultados de una valoración de los riesgos ayudarán a guiar y a determinar la acción de gestión apropiada y las prioridades para la gestión de los riesgos de seguridad de la información, y para la implementación de los controles seleccionados para protegerse contra estos riesgos.

La norma ISO/IEC 27005[11] brinda orientación sobre gestión de riesgos de seguridad de la información, e incluye asesoría sobre valoración, tratamiento, aceptación, comunicación, seguimiento y revisión de riesgos.

0.3 SELECCIÓN DE CONTROLES

Los controles se pueden seleccionar de esta guía o de otros grupos de control, o se pueden diseñar nuevos controles para satisfacer necesidades específicas.

La selección de controles depende de las decisiones organizacionales basadas en los criterios para la aceptación de riesgos, las opciones para tratamiento de riesgos y el enfoque general para la gestión de riesgos aplicado a la organización, y debería estar sujeta a toda la legislación y reglamentación nacionales e internacionales pertinentes. La selección de los controles también depende de la forma en la que los controles interactúan para defender en profundidad.

Algunos de los controles de esta guía se pueden considerar como principios de orientación para gestión de la seguridad de la información y aplicables a la mayoría de organizaciones. Los

controles se explican con más detalle más adelante, junto con la guía de implementación. En la norma ISO/IEC 27005[11] se puede encontrar más información acerca de la selección de controles y de otras opciones para tratamiento de riesgos.

0.4 DESARROLLO DE SUS PROPIAS DIRECTRICES

Esta guía se puede considerar como un punto de partida para el desarrollo de directrices específicas de la organización. No todos los controles y orientación de este código de práctica pueden ser aplicables. Además, se pueden requerir controles y directrices adicionales que no están incluidos en esta guía. Cuando los documentos que se desarrollan contienen directrices o controles adicionales, puede ser útil incluir referencias cruzadas a los numerales de esta guía, en donde sea aplicable, para facilitar la verificación del cumplimiento por parte de los auditores y socios de negocios.

0.5 CONSIDERACIONES SOBRE EL CICLO DE VIDA

La información tiene un ciclo de vida natural, desde su creación y origen, pasando por el almacenamiento, procesamiento, uso y transmisión, hasta su deterioro o destrucción final. El valor de los activos y los riesgos para los activos pueden variar durante su ciclo de vida (por ejemplo, la divulgación no autorizada o el robo de las cuentas financieras de una compañía es mucho menos significativa después de que se han publicado formalmente), pero la seguridad de la información sigue siendo importante en todas las etapas, en alguna medida.

Los sistemas de información tienen ciclos de vida dentro de los cuales se lleva a cabo su concepción, especificación, diseño, desarrollo, pruebas, implementación, uso, mantenimiento y finalmente el retiro de servicio y su disposición. La seguridad de la información se debería tener en cuenta en todas las etapas. Los nuevos desarrollos de sistemas y los cambios en los sistemas existentes presentan oportunidades para que las organizaciones actualicen y mejoren sus controles de seguridad, teniendo en cuenta los incidentes reales y los riesgos de seguridad de la información presentes y proyectados.

0.6 NORMAS RELACIONADAS

Aunque esta guía ofrece orientación sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones, las otras normas de la familia ISO/IEC 27000 brindan asesoría o requisitos complementarios sobre otros aspectos del proceso total de gestión de seguridad de la información.

Consulte la norma ISO/IEC 27000, que presenta una introducción general al SGSI y a la familia de normas. La norma ISO/IEC 27000 presenta un glosario que define formalmente la mayoría de términos usados en la familia de normas ISO/IEC 27000, y describe el objeto, campo de aplicación y los objetivos de cada miembro de la familia.

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETO Y CAMPO DE APLICACIÓN

La presente Guía proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, teniendo en cuenta el(los) entorno(s) del riesgo de seguridad de la información de la organización.

Esta Guía está diseñada por organizaciones que tienen el propósito de:

a) seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información con base en la norma NTC-ISO/IEC 27001[10];

b) implementar controles de seguridad de la información comúnmente aceptados;

c) desarrollar sus propias directrices de gestión de la seguridad de la información.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

ISO/IEC 27000, *Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.*

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

4. ESTRUCTURA DE ESTA GUIA

Esta guía contiene 14 numerales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.

4.1 NUMERALES

Cada numeral que define controles de seguridad contiene una o más categorías de seguridad principales.

El orden de los numerales en esta guía no tiene que ver con su importancia. Dependiendo de las circunstancias, los controles de seguridad de alguno o de todos los numerales pueden ser importantes; por tanto, cada organización que aplica esta guía debería identificar los controles aplicables, su grado de importancia y su aplicación a los procesos individuales del negocio. Además, las listas de esta guía no se presentan en orden de prioridad.

4.2 CATEGORÍAS DE CONTROL

Cada categoría principal de control de la seguridad contiene:

a) un objetivo de control que establece lo que se va a lograr;

b) uno o más controles que se pueden aplicar para lograr el objetivo de control.

Las descripciones de los controles están estructuradas de la siguiente manera:

Control

Define la declaración específica del control para satisfacer el objetivo del control.

Guía de implementación

Brinda información más detallada para apoyar la implementación del control y cumplir el objetivo del control. Es posible que la orientación no sea completamente adecuada ni suficiente en todas las situaciones, y que no cumpla los requisitos de control específicos de la organización.

Información adicional

Brinda información adicional que puede ser necesario considerar, por ejemplo, las consideraciones legales y referencias a otras normas. Si no hay información adicional que suministrar, no se incluye esta parte.

5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

5.1.1 Políticas para la seguridad de la información

Control

Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

Guía de implementación

Desde el más alto nivel, las organizaciones deberían definir una "política de seguridad de la información" que sea aprobada por la dirección y que establezca el enfoque de la organización para la gestión de sus objetivos de seguridad de la información.

Las políticas de la seguridad de la información deberían abordar los requisitos creados por:

a) estrategia de negocio;

b) reglamentaciones, legislación y contratos;

c) el entorno actual y proyectado de amenazas a la seguridad de la información.

La política de la seguridad de la información debería contener declaraciones concernientes a:

a) la definición de seguridad de la información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información;

b) la asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;

c) procesos para manejar desviaciones y excepciones.

Desde el más bajo nivel, la política de la seguridad de la información debería estar apoyada en políticas específicas por temas, que además exigen la implementación de controles de seguridad de la información y están típicamente estructuradas para tener en cuenta las necesidades de algunos grupos objetivo dentro de una organización, o para tener en cuenta temas determinados.

Algunos ejemplos de estos temas de políticas incluyen:

a) control de acceso (véase el numeral 9);

b) clasificación de la información (véase el numeral 8.2);

c) seguridad física y del entorno (véase el numeral 11);

d) temas orientados a los usuarios finales, tales como:

   1) uso aceptable de los activos (véase el numeral 8.1.3);

   2) política de escritorio y pantalla limpia (véase el numeral 11.2.9);

   3) transferencia de información (véase el numeral 13.2.1);

   4) dispositivos móviles y teletrabajo (véase el numeral 6.2);

   5) restricciones sobre instalaciones y uso del software (véase el numeral 12.6.2);

e) copias de respaldo (véase el numeral 12.3);

f) transferencia de información (véase el numeral 13.2);

g) protección contra códigos maliciosos (véase el numeral 12.2);

h) gestión de las vulnerabilidades técnicas (véase el numeral 12.6.1);

i) controles criptográficos (véase el numeral 10);

j) seguridad de las comunicaciones (véase el numeral 13);

k) privacidad y protección de información de datos personales (véase el numeral 18.1.4);

l) relaciones con los proveedores (véase el numeral 15);

Estas políticas se deberían comunicar a los empleados y a las partes externas interesadas, en una forma que sea pertinente, accesible y comprensible para el lector previsto, por ejemplo, en el contexto de un "programa de toma de conciencia, educación y formación en la seguridad de la información" (véase el numeral 7.2.2).

Información adicional

La necesidad de políticas internas para la seguridad de la información varía a través de las organizaciones. Las políticas internas son especialmente útiles en organizaciones de mayor tamaño y complejidad, en donde las políticas que definen y aprueban los niveles esperados de control están separadas de las que implementan los controles, o en situaciones en las que una política se aplica a muchas personas o funciones diferentes en la organización. Las políticas para seguridad de la información se pueden publicar en un solo documento de "política de la seguridad de la información" o como un conjunto de documentos individuales pero relacionados.

Si alguna de las políticas de seguridad de la información se distribuye por fuera de la organización, se debería tener cuidado de no revelar información confidencial.

Algunas organizaciones usan otros términos para designar estos documentos de políticas, tales como "Normas", Directivas" o "Reglas".

5.1.2 Revisión de las políticas para la seguridad de la información

Control

Las políticas para la seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

Guía de implementación

Cada política debería tener un propietario que tenga la responsabilidad aprobada por la dirección, para el desarrollo, revisión y evaluación de las políticas. La revisión debería incluir la valoración de las oportunidades de mejora de las políticas de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno organizacional, las circunstancias del negocio, las condiciones legales o el ambiente técnico.

La revisión de las políticas para seguridad de la información debería tener en cuenta los resultados de las revisiones por la dirección.

Se debería obtener la aprobación de la dirección con relación a una política revisada.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 ORGANIZACIÓN INTERNA

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

6.1.1 Roles y responsabilidades para la seguridad de la información

Control

Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.

Guía de implementación

La asignación de las responsabilidades de seguridad de la información se debería hacer de acuerdo con las políticas para la seguridad de la información (véase el numeral 5.1.1). Se deberían identificar las responsabilidades para la protección de los activos individuales y para llevar a cabo procesos de seguridad de la información específicos. Se deberían definir las responsabilidades para las actividades de gestión del riesgo de la seguridad de la información, y en particular, para la aceptación de riesgos residuales. Cuando sea necesario, estas responsabilidades se deberían complementar con orientación detallada para sitios e instalaciones de procesamiento de información específicos. Se deberían definir las responsabilidades locales para la protección de activos y para la realización de procesos de seguridad específicos.

Los individuos a los que se les ha asignado responsabilidades de seguridad de la información pueden delegar a otros las tareas de seguridad de la información. No obstante, siguen siendo responsables y deberían determinar la ejecución correcta de cualquier tarea delegada.

Se deberían establecer las áreas de las cuales son responsables los individuos. En particular, se debería efectuar lo siguiente:

a) se deberían identificar y definir los activos y los procesos de seguridad de la información;

b) se debería asignar la entidad responsable de cada activo o proceso de seguridad de la información, y se deberían documentar los detalles de esta responsabilidad (véase el numeral 8.1.2);

c) se deberían definir y documentar los niveles de autorización;

d) para tener la capacidad de cumplir las responsabilidades en el área de seguridad de la información, los individuos nombrados deberían ser competentes en el área y se les debería brindar oportunidades de mantenerse actualizados con los avances en este tema;

e) se deberían identificar y documentar la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores.

Información adicional

Muchas organizaciones nombran un gerente de seguridad de la información que asuma la responsabilidad total por el desarrollo e implementación de la seguridad de la información y que apoye la identificación de los controles.

Sin embargo, la responsabilidad por la obtención de recursos y la implementación de controles será con frecuencia de los gerentes individuales. Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección diaria.

6.1.2 Segregación de funciones

Control

Las funciones y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

Guía de implementación

Es conveniente prestar atención a que ninguna persona pueda acceder, modificar o usar activos sin autorización ni detección. El inicio de un evento debería estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación

Para las organizaciones pequeñas la segregación de funciones puede ser difícil de lograr, pero el principio se debería aplicar en tanto sea posible y viable. Siempre que resulte difícil hacer la segregación, se deberían considerar otros controles, tales como el seguimiento de actividades, los rastros de auditoría (*Audit Trails*) y la supervisión de la dirección.

Información adicional

La segregación de funciones es un método para reducir el uso indebido, accidental o deliberado, de los activos de una organización.

6.1.3 Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de regulación y las autoridades de supervisión), y cómo se deberían reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).

Información adicional

Las organizaciones que son atacadas por Internet pueden necesitar que las autoridades emprendan acciones contra la fuente del ataque.

El mantenimiento de estos contactos puede ser un requisito para apoyar la gestión de incidentes de seguridad de la información (véase el numeral 16) o el proceso de continuidad de negocio, o el proceso de planificación de contingencias (véase el numeral 17). Los contactos con organismos de regulación son útiles para anticiparse y prepararse para los cambios inminentes en las leyes o reglamentaciones que la organización ha de implementar. Los contactos con otras autoridades incluyen las empresas de servicio públicos, los servicios de emergencia, los proveedores de electricidad y de salud y seguridad, por ejemplo, los

departamentos de bomberos (en relación con la continuidad de negocio), los proveedores de telecomunicaciones (en relación con la disponibilidad y enrutamiento de líneas) y los proveedores de agua (en relación con las instalaciones de enfriamiento de equipos).

6.1.4 Contacto con grupos de interés especial

Control

Se debería mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Guía de implementación

La membrecía en grupos o foros de interés especial se debería considerar como un medio para:

a) mejorar el conocimiento acerca de las mejores prácticas y permanecer al día con la información de seguridad pertinente;

b) asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa;

c) recibir advertencias tempranas de las alertas, avisos y parches acerca de ataques y vulnerabilidades;

d) obtener acceso a asesoría especializada en seguridad de la información;

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

f) brindar puntos de enlace adecuados cuando se trata con incidentes de seguridad de la información (véase el numeral 16).

Información adicional

Se pueden establecer acuerdos acerca de intercambio de información para mejorar la cooperación y coordinación de cuestiones de seguridad. Estos acuerdos deberían identificar los requisitos para la protección de información confidencial.

6.1.5 Seguridad de la información en la gestión de proyectos

Control

La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.

Guía de implementación

La seguridad de la información se debería integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte. Los métodos de gestión de proyectos que se usen deberían requerir que:

a) los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto;

b) la valoración de los riesgos de seguridad de la información se lleva a cabo en una etapa temprana del proyecto, para identificar los controles necesarios;

c) la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

Las implicaciones de la seguridad de la información se deberían tener en cuenta y revisar en forma regular en todos los proyectos. Se deberían definir las responsabilidades para seguridad de la información, y asignarlas a roles especificados definidos en los métodos de gestión de proyectos.

6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política para dispositivos móviles

Control

Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Guía de implementación

Cuando se usan dispositivos móviles, se debería prestar atención especial a asegurar que no se comprometa la información del negocio. La política de dispositivos móviles debería tener en cuenta los riesgos de trabajar con dispositivos móviles en entornos no protegidos.

La política de dispositivos móviles debería considerar:

a) el registro de los dispositivos móviles;

b) los requisitos de la protección física;

c) las restricciones para la instalación de software;

d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches;

e) la restricción de la conexión a servicios de información;

f) controles de acceso;

g) técnicas criptográficas;

h) protección contra software malicioso;

i) deshabilitación remota, borrado o cierre

j) copias de respaldo;

k) uso de servicios y aplicaciones web.

Se debería tener cuidado cuando se usan dispositivos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas. Se debería contar con protección para evitar el acceso o la divulgación no autorizada de la información almacenada y procesada por estos dispositivos, por ejemplo, usando técnicas criptográficas (véase el numeral 10) e imponiendo el uso de información secreta para la autenticación (véase el numeral 9.2.4).

Los dispositivos móviles también deberían estar protegidos físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones. Se debería establecer un procedimiento específico teniendo en cuenta los requisitos legales, de seguros y otros requisitos de seguridad de la organización, para los casos de robo o pérdida de dispositivos móviles. Los dispositivos que contienen información importante, sensible o crítica para el negocio no se deberían dejar sin supervisión, y donde sea posible, deberían estar encerrados bajo llave o se deberían usar cerraduras especiales para asegurarlos.

Se debería disponer de entrenamiento para el personal que usa dispositivos móviles, para incrementar el nivel de concienciación sobre los riesgos adicionales que resultan de este tipo de trabajo, y los controles que se deberían implementar.

Cuando la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas también deberían considerar:

a) la separación entre el uso privado y de negocio de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del negocio en un dispositivo privado;

b) brindar acceso a la información del negocio solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos del negocio, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el servicio. Esta política necesita tener en cuenta la legislación sobre privacidad.

Información adicional

Las conexiones inalámbricas para dispositivos móviles son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se deberían considerar cuando se identifican controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbricos no están desarrollados suficientemente, y tienen debilidades conocidas;

b) es posible que la información almacenada en los dispositivos móviles no esté copiada en discos de respaldo debido a limitaciones en el ancho de banda o porque los dispositivos móviles no estén conectados en los tiempos en que se programa la elaboración de copias de respaldo.

Los dispositivos móviles generalmente comparten funciones comunes con los dispositivos de uso fijo, por ejemplo, trabajo en red, acceso a internet, correo electrónico y manejo de archivos. Los controles de seguridad de la información para los dispositivos móviles generalmente consisten en los controles adoptados en los dispositivos de uso fijo, y en los controles para tratar las amenazas que surgen por su uso fuera de las instalaciones de la organización.

6.2.2 Teletrabajo

Control

Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Guía de implementación

Las organizaciones que permiten actividades de teletrabajo deberían expedir una política que defina las condiciones y restricciones para el uso del teletrabajo. Cuando se considera aplicable y lo permite la ley, se deberían considerar los siguientes asuntos:

a) la seguridad física existente en el sitio del teletrabajo, teniendo en cuenta la seguridad física de la edificación y del entorno local;

b) el entorno físico 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 sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno;

d) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada;

e) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos;

f) el uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica;

g) las políticas y procedimientos para evitar conflictos relacionados con los derechos de propiedad intelectual sobre desarrollos realizados en equipos de propiedad privada;

h) el acceso a equipo de propiedad privada (para verificar su seguridad o como parte de una investigación), el cual puede ser prohibido por la legislación;

i) acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos;

j) requisitos de firewall y de protección contra software malicioso.

Las directrices y acuerdos que se consideren deberían incluir:

a) el suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización;

b) una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder;

c) el suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto;

d) seguridad física;

e) las reglas y orientación sobre el acceso de la familia y los visitantes a los equipos y a la información;

f) el suministro de soporte y mantenimiento del hardware y el software;

g) el suministro de seguros;

h) los procedimientos para copias de respaldo y continuidad del negocio;

i) auditoría y seguimiento de la seguridad;

j) la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.

Información adicional

El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".

7. SEGURIDAD DEL RECURSO HUMANO

7.1 ANTES DE ASUMIR EL EMPLEO

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

7.1.1 Selección

Control

Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

Guía de implementación

La verificación debería tener en cuenta todo lo relacionado con la privacidad, la protección de la información de datos personales y la legislación laboral, y cuando se permita, debería incluir lo siguiente:

a) la disponibilidad de referencias satisfactorias, por ejemplo, una comercial y una personal;

b) una verificación (completa y precisa) de la hoja de vida del solicitante;

c) confirmación de las calificaciones académicas y profesionales declaradas;

d) una verificación de identidad independiente (pasaporte o documento similar);

e) una verificación más detallada, como la de la información crediticia o de antecedentes penales.

Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato:

a) tenga la competencia necesaria para desempeñar el rol de seguridad;

b) sea confiable para desempeñar el rol, especialmente si es crítico para la organización.

Cuando un trabajo, ya sea por nombramiento o promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y limitantes para las revisiones de verificación, por ejemplo, quién es elegible para seleccionar a las personas, y cómo, cuándo y por qué se llevan a cabo revisiones de verificación.

También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud.

La información de todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la legislación existente. Dependiendo de la legislación aplicable, se debería informar de antemano a los candidatos acerca de las actividades de selección.

7.1.2 Términos y condiciones del empleo

Control

Los acuerdos contractuales con empleados y contratistas deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Guía de implementación

Las obligaciones contractuales para empleados o contratistas, deberían reflejar las políticas de la organización en cuanto a seguridad de la información, y además deberían aclarar y establecer:

a) que todos los empleados y contratistas a los que se brinde acceso a información confidencial deberían firmar un acuerdo de confidencialidad y no divulgación, antes de tener acceso a las instalaciones de procesamiento de información (véase el numeral 13.2.4);

b) las responsabilidades y derechos legales de empleados o contratistas, por ejemplo, con relación a leyes sobre derecho de autor o legislación sobre protección de datos (véanse los numerales 18.1.2 y 18.1.4);

c) las responsabilidades para la clasificación de la información y la gestión de información organizacional y otros activos asociados con información, instalaciones de procesamiento de información y servicios de información manejados por el empleado o contratista (véase el numeral 8);

d) las responsabilidades del empleado o contratista para el manejo de la información recibida de otras compañías o partes externas;

e) las acciones por tomar, si el empleado o contratista no tiene en cuenta los requisitos de seguridad de la organización (véase el numeral 7.2.3).

Los roles y responsabilidades de seguridad de la información se deberían comunicar a los candidatos al empleo, durante el proceso previo a la vinculación.

La organización se debería asegurar de que los empleados y contratistas acepten los términos y condiciones relativos a la seguridad de la información, referente a la naturaleza y al alcance del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas dentro de los términos y condiciones del empleo deberían continuar durante un período definido después de finalizado el empleo (véase el numeral 7.3).

Información adicional

Se puede usar un código de conducta para establecer las responsabilidades de seguridad de la información del empleado o del contratista acerca de confidencialidad, protección de datos, ética, uso apropiado de los equipos e instalaciones de la organización, al igual que las prácticas formales esperadas por la organización. A una parte externa, con la cual está asociado un contratista, se le puede pedir que establezca acuerdos contractuales en nombre del individuo contratado.

7.2 DURANTE LA EJECUCIÓN DEL EMPLEO

Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

7.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir asegurarse de que los empleados y contratistas:

a) estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales;

b) se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la organización;

c) estén motivados para cumplir las políticas de seguridad de la información de la organización;

d) logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización (véase el numeral 7.2.2);

e) cumplan los términos y las condiciones del empleo, que incluyen la política de seguridad de la información y los métodos de trabajo apropiados;

f) tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular;

g) cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).

La dirección debería demostrar apoyo a las políticas, procedimientos y controles de seguridad de la información, y actuar como un modelo a seguir.

Información adicional

Si los empleados y contratistas no toman conciencia de sus responsabilidades de seguridad de la información, pueden causar un daño considerable a una organización. El personal motivado tiende a ser más confiable y a causar menos incidentes de seguridad de la información.

Una gestión deficiente puede hacer que el personal se sienta subvalorado, lo que da como resultado un impacto negativo de la seguridad de la información sobre la organización. Por ejemplo, una gestión deficiente puede conducir a que se descuide la seguridad de la información o a que se usen en forma indebida los activos de la organización.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Control

Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Guía de implementación

Un programa de toma de conciencia en seguridad de la información, debería apuntar a que los empleados, y en donde sea pertinente, los contratistas, tomen conciencia de sus responsabilidades de seguridad de la información, y de los medios por los cuales se cumplen estas responsabilidades.

Se debería establecer un programa de toma de conciencia en seguridad de la información, en línea con las políticas y procedimientos pertinentes de seguridad de la información de la organización, teniendo en cuenta la información de la organización que se va proteger, y los controles que se han implementado para proteger la información. El programa de toma de conciencia debería incluir varias actividades para toma de conciencia, tales como campañas (por ejemplo, el “día de la seguridad de la información”) y la elaboración de folletos y boletines de noticias.

El programa de toma de conciencia se debería planificar teniendo en cuenta los roles de los empleados en la organización, y en donde sea pertinente, la expectativa de la organización con

relación a la toma de conciencia de los contratistas. Las actividades del programa de toma de conciencia se deberían programar en el tiempo, de preferencia con regularidad, de manera que las actividades se repitan y abarquen a nuevos empleados y contratistas. El programa de toma de conciencia también se debería actualizar regularmente, de manera que permanezca en línea con las políticas y procedimientos organizacionales, y se debería construir con base en las lecciones aprendidas de incidentes de seguridad de la información.

La formación en toma de conciencia se debería llevar a cabo según lo requiera el programa de toma de conciencia en seguridad de la información de la organización. Para la formación en toma de conciencia se pueden usar diferentes medios, incluyendo clase en aula, aprendizaje a distancia, aprendizaje basado en la web, aprendizaje autónomo, y otros.

La educación y la formación en seguridad de la información también deberían comprender aspectos generales tales como:

a) la declaración del compromiso de la dirección con la seguridad de la información en toda la organización;

b) la necesidad de conocer y cumplir con las reglas y obligaciones de seguridad de la información aplicables, tal como se definen en las políticas, normas, leyes, reglamentos, contratos y acuerdos;

c) la rendición personal de cuentas por las acciones y omisiones propias, y las responsabilidades generales relacionadas con la seguridad y la protección de la información que pertenece a la organización y a las partes externas;

d) los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios);

e) los puntos de contacto y los recursos para información adicional y asesoría sobre asuntos de seguridad de la información, incluidos los materiales de educación y formación sobre seguridad de la información.

La educación y la formación en seguridad de la información se deberían llevar a cabo periódicamente. La educación y entrenamiento iniciales aplican a quienes se transfieren a nuevos cargos o roles con requisitos de seguridad de la información considerablemente diferentes, no solo para los nuevos empleados, y se deberían llevar a cabo antes de que se active el rol.

La organización debería desarrollar el programa de educación y de formación para impartir la educación y la formación eficazmente. El programa debería estar en línea con las políticas y procedimientos pertinentes de seguridad de la información de la organización, teniendo en cuenta la información de la organización que se va a proteger, y los controles que se han implementado para proteger la información. El programa debería considerar diferentes formas de educación y formación, por ejemplo, conferencias o estudio autónomo.

Información adicional

Cuando se prepara un programa de toma de conciencia es importante enfocarse no solamente en el “qué” y en el “cómo” sino también en el “por qué”. Es importante que los empleados comprendan el objetivo de la seguridad de la información y el impacto potencial, positivo y negativo, que tiene su propio comportamiento para la organización.

La toma de conciencia, la educación y la formación pueden ser parte de otras actividades de formación, por ejemplo, formación general en seguridad o en TI, o se pueden llevar a cabo en colaboración con ellas. Las actividades de toma de conciencia, educación y formación deberían ser adecuadas y pertinentes a los roles, responsabilidades y habilidades de los individuos.

Al finalizar el curso de formación, educación y toma de conciencia, se puede llevar a cabo una evaluación de la comprensión de los empleados para comprobar la transferencia de conocimiento.

7.2.3 Proceso disciplinario

Control

Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Guía de implementación

El proceso disciplinario no se debería iniciar sin antes verificar que ha ocurrido una violación a la seguridad de la información (véase el numeral 16.1.7).

El proceso disciplinario formal debería asegurar el tratamiento correcto e imparcial a los empleados de quienes se sospecha que han cometido violaciones a la seguridad de la información. El proceso disciplinario formal debería proveer una respuesta gradual que tenga en cuenta factores tales como la naturaleza y la gravedad de la violación y su impacto sobre el negocio; si es o no su primera infracción; si el infractor tenía la formación apropiada; la legislación pertinente; los contratos del negocio y otros factores, según se requiera.

El proceso disciplinario también se debería usar como un elemento disuasivo para prevenir que los empleados violen las políticas y procedimientos de seguridad de la información de la organización, y de cualquier otra violación a la seguridad de la información. Las violaciones deliberadas pueden requerir acciones inmediatas.

Información adicional

El proceso disciplinario también se puede convertir en una motivación, o en un incentivo, si se definen sanciones positivas para un comportamiento destacado con relación a la seguridad de la información.

7.3 TERMINACIÓN Y CAMBIO DE EMPLEO

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

7.3.1 Responsabilidades en la Terminación o cambio del empleo

Control

Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.

Guía de implementación

La comunicación de las responsabilidades en la terminación debería incluir los requisitos de seguridad de la información y las responsabilidades legales vigentes, y en donde sea apropiado, las responsabilidades contenidas en cualquier acuerdo de confidencialidad (véase el numeral 13.2.4) y los términos y condiciones del empleo (véase el numeral 7.1.2) que continúan después de un período definido, luego de finalizar el empleo del contratista o del empleado.

Las responsabilidades y deberes que siguen siendo válidos después de la terminación del empleo, deberían estar contenidos en los términos y condiciones del empleo del empleado o del contratista (véase el numeral 7.1.2).

Los cambios de responsabilidad o de empleo se deberían manejar como la terminación de la responsabilidad o empleo actual, combinada con el inicio de una nueva responsabilidad o empleo.

Información adicional

Generalmente, Recursos Humanos es responsable del proceso total de terminación del empleo y trabaja en conjunto con el supervisor a cargo de la persona que se retira, para gestionar los aspectos de seguridad de la información de los procedimientos relevantes. En el caso de un contratista suministrado a través de una parte externa, este proceso de terminación lo lleva a cabo dicha parte, de acuerdo con el contrato suscrito entre la organización y la parte externa.

Puede ser necesario informar a los empleados, clientes o contratistas acerca de los cambios de personal y de las disposiciones operativas.

8. GESTIÓN DE ACTIVOS

8.1 RESPONSABILIDAD POR LOS ACTIVOS

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

8.1.1 Inventario de activos

Control

Se deberían identificar la información, otros activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Guía de implementación

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información, y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. La documentación se debería mantener en inventarios dedicados o existentes, según sea apropiado.

El inventario de activos debería ser exacto, actualizado, consistente y alineado con otros inventarios.

Para cada uno de los activos identificados, se debería asignar la propiedad del activo (véase el numeral 8.1.2) y se debería identificar la clasificación (véase el numeral 8.2).

Información adicional

Los inventarios de activos ayudan a asegurar que se cuenta con una protección efectiva, y también pueden ser necesarios para otros propósitos, como por ejemplo razones de salud y seguridad, seguros o asuntos financieros (gestión de activos).

La norma ISO/IEC 27005[11] proporciona ejemplos de activos que la organización podría tener que considerar cuando se identifican los activos. El proceso de elaborar un inventario de activos es un prerrequisito importante de la gestión del riesgo (véanse también las normas ISO/IEC 27000 e ISO/IEC 27005[11]).

8.1.2 Propiedad de los activos

Control

Los activos mantenidos en el inventario deberían tener un propietario.

Guía de implementación

Los individuos, así como otras entidades con la responsabilidad delegada sobre la gestión del activo dentro de su ciclo de vida, califican para ser asignados como propietarios de los activos.

Usualmente se implementa un proceso para asegurar la asignación oportuna de la propiedad de los activos. La propiedad se debería asignar cuando los activos se crean o cuando son transferidos a la organización. El propietario de un activo debería ser responsable de su gestión apropiada durante todo su ciclo de vida.

El propietario del activo debería:

a) asegurarse de que los activos están inventariados;

b) asegurarse de que los activos están clasificados y protegidos apropiadamente;

c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables;

d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

Información adicional

El propietario identificado puede ser un individuo o una entidad que tenga la responsabilidad delegada sobre la gestión para controlar todo el ciclo de vida de un activo. El propietario identificado no necesariamente tiene algún derecho de propiedad sobre el activo.

Las tareas de rutina pueden ser delegadas, por ejemplo, a un custodio que vela por los activos diariamente, pero la responsabilidad sigue siendo del propietario.

En sistemas de información complejos, puede ser útil designar grupos de activos que actúan conjuntamente para brindar un servicio particular. En este caso, el propietario de este servicio rinde cuentas por la prestación del servicio, incluida la operación de sus activos.

8.1.3 Uso aceptable de los activos

Control

Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Guía de implementación

Los empleados y usuarios de partes externas que usan activos de la organización o tienen acceso a ellos deberían tomar conciencia de los requisitos de seguridad de la información de la organización, de los activos de la organización asociados con información y con instalaciones y recursos de procesamiento de información. Deberían ser responsables del uso que hacen de cualquier recurso de procesamiento de la información, y de cualquier uso ejecutado bajo su responsabilidad.

8.1.4 Devolución de activos

Control

Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Guía de implementación

El proceso de terminación se debería formalizar para incluir la devolución de todos los activos físicos y electrónicos entregados previamente, que son propiedad de la organización o que se le han confiado a ella.

En los casos en que el empleado o parte externa compre el equipo de la organización o use su propio equipo personal, se deberían seguir procedimientos para asegurar que toda la información pertinente sea transferida a la organización y borrada del equipo en forma segura (véase el numeral 11.2.7).

En los casos en que un empleado o usuario de una parte externa tenga conocimientos que son importantes para las operaciones en curso, esa información se debería documentar y transferir a la organización.

Durante el período de notificación de la terminación, la organización debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control

La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Guía de implementación

Las clasificaciones y controles de protección de información asociados deberían tener en cuenta las necesidades del negocio en cuanto a intercambio o restricción de información, al igual que los requisitos legales. Los activos diferentes de información también se pueden clasificar de conformidad con la clasificación de la información que se almacena, procesa maneja o protege el activo.

Los propietarios de los activos de información deberían rendir cuentas por su clasificación.

El esquema de clasificación debería incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación en el tiempo. El nivel de protección en el esquema se debería evaluar analizando la confidencialidad, la integridad y la disponibilidad, y cualquier otro requisito para la información considerada. El esquema se debería alinear con la política de control de acceso (véase el numeral 9.1.1).

Cada nivel debería recibir un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.

El esquema debería ser consistente a lo largo y ancho de la organización, de manera que todos clasifiquen la información y los activos relacionados de la misma manera, tengan una comprensión común de los requisitos de protección, y apliquen la protección apropiada.

La clasificación se debería incluir en los procesos de la organización, y debería ser consistente y coherente en toda la organización. Los resultados de la clasificación deberían indicar el valor de los activos dependiendo de su sensibilidad y criticidad para la organización, por ejemplo, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación se deberían actualizar de acuerdo con los cambios en su valor, sensibilidad y criticidad durante el ciclo de vida.

Información adicional

La clasificación brinda a las personas que tratan con información, una indicación concisa de cómo manejarla y protegerla. Esto se facilita mediante la creación de grupos de información con necesidades de protección similares, y la especificación de procedimientos que se apliquen a toda la información en cada grupo. Este enfoque reduce la necesidad de valorar los riesgos caso por caso, y de diseñar controles a la medida.

La información puede dejar de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos se deberían tener en cuenta, ya que la clasificación excesiva puede conducir a la implementación de controles innecesarios que generan gastos adicionales, o por el contrario, clasificación deficiente que pone en peligro el logro de los objetivos del negocio.

Un ejemplo del esquema de clasificación de la confidencialidad de la información se puede basar en los cuatro niveles siguientes:

a) la divulgación no causa daño;

b) la divulgación causa algo de vergüenza o un inconveniente operativo menor;

c) la divulgación tiene un impacto significativo a corto plazo en las operaciones u objetivos tácticos;

d) la divulgación tiene un serio impacto en los objetivos estratégicos a largo plazo, o pone en riesgo la supervivencia de la organización.

8.2.2 Etiquetado de la información

Control

Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Guía de implementación

Los procedimientos para el etiquetado de información necesitan abarcar la información y sus activos relacionados en formatos físicos y electrónicos. El etiquetado debería reflejar el esquema de clasificación establecido en el numeral 8.2.1. Las etiquetas se deberían poder reconocer fácilmente. Los procedimientos deberían brindar orientación acerca de dónde y cómo se colocan las etiquetas, teniendo en cuenta la forma en que se obtiene el acceso a la información o se manejan los activos, dependiendo de los tipos de medio. Los procedimientos pueden definir casos en los que se omite el etiquetado, por ejemplo, el etiquetado de información no confidencial para reducir cargas de trabajo. Los empleados y contratistas deberían tomar conciencia de los procedimientos de etiquetado.

Las salidas de los sistemas que contienen información que se clasifica como sensible o crítica debería portar una etiqueta de clasificación apropiada.

Información adicional

El etiquetado de la información clasificada es un requisito clave para las disposiciones sobre intercambio de información. Las etiquetas físicas y los metadatos son una forma común de etiquetado.

El etiquetado de la información y de sus activos relacionados algunas veces tiene efectos negativos. Los activos clasificados son más fáciles de identificar, y en consecuencia, más fáciles de ser hurtados por atacantes internos o externos.

8.2.3 Manejo de activos

Control

Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Guía de implementación

Se deberían elaborar procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación (véase el numeral 8.2.1).

Se deberían considerar los siguientes asuntos:

a) las restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación;

b) el mantenimiento de un registro formal de los receptores autorizados de los activos;

c) la protección de copias temporales o permanentes de información a un nivel coherente con la protección de la información original;

d) el almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes;

e) el marcado claro de todas las copias de medios para el cuidado del receptor autorizado.

Es posible que el esquema de clasificación usado en la organización no sea equivalente a los esquemas usados por otras organizaciones, aunque sus nombres sean similares; además, la información que se transfiere entre las organizaciones puede variar en su clasificación, dependiendo de su contexto en cada organización, aun cuando sus esquemas de clasificación sean idénticos.

Los acuerdos con otras organizaciones que incluyan intercambio de información deberían incluir procedimientos para identificar la clasificación de esa información y para interpretar las etiquetas de clasificación de otras organizaciones.

8.3 MANEJO DE MEDIOS

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

8.3.1 Gestión de medios removibles

Control

Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

Guía de implementación

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

a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debería remover de forma que no sea recuperable;

b) cuando resulte necesario y práctico, se debería solicitar autorización para retirar los medios de la organización, y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría (*Audit Trail*);

c) todos los medios se deberían almacenar en un ambiente protegido y seguro, de acuerdo con las especificaciones de los fabricantes;

d) si la confidencialidad o integridad de los datos se consideran importantes, se deberían usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles;

e) para mitigar el riesgo de degradación de los medios mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios diferentes antes de que se vuelvan ilegibles;

f) se deberían guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida simultánea de los datos;

g) se debería considerar el registro de los medios removibles para reducir la oportunidad de pérdida de datos;

h) sólo se deberían habilitar unidades de medios removibles si hay una razón de negocio para hacerlo;

i) en donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios.

Los procedimientos y niveles de autorización se deberían documentar.

8.3.2 Disposición de los medios

Control

Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.

Guía de implementación

Se deberían establecer procedimientos formales para la disposición segura de los medios, para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la disposición segura de los medios que contienen información confidencial deberían ser proporcionales a lo sensible de esa información. Se deberían considerar los siguientes asuntos:

a) los medios que contienen información confidencial se deberían almacenar y disponer en forma segura, por ejemplo, mediante incineración, destrucción, o el borrado de datos antes de ser usado por otra aplicación dentro de la organización;

b) se debería contar con procedimientos para identificar los elementos que podrían requerir su disposición segura;

c) puede ser más fácil hacer arreglos para todos los medios que se van a recolectar y disponerlos en forma segura, que intentar separarlos de los elementos críticos

d) muchas organizaciones ofrecen servicios de recolección y disposición de medios; es conveniente seleccionar cuidadosamente una parte externa adecuada, con controles y experiencia adecuados;

e) la disposición de los elementos críticos se debería registrar (*Logged*) con el fin de mantener un rastro de auditoría (*Audit Trail*).

Cuando se acumulan los medios para su disposición, se debería tener en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se vuelva sensible.

Información adicional

Los dispositivos dañados que contienen datos sensibles pueden requerir una valoración de riesgos para determinar si los elementos se deberían destruir físicamente en vez de enviarlos a reparación o desecharlos (véase el numeral 11.2.7).

8.3.3 Transferencia de medios físicos

Control

Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Guía de implementación

Las siguientes directrices se deberían considerar para la protección de medios que contienen información, durante el transporte:

a) se debería usar un transporte o servicios de mensajería confiables;

b) se debería acordar con la dirección una lista de servicios de mensajería autorizados;

c) se deberían desarrollar procedimientos para verificar la identificación de los servicios de mensajería;

d) el embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos;

e) se debería llevar un registro (*Logs*) que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

Información adicional

La información puede ser vulnerable al acceso no autorizado, al uso indebido o corrupción durante el transporte físico, por ejemplo, cuando se envía por el servicio postal o por un servicio de mensajería. En este control, los medios incluyen documentos en papel.

Cuando la información confidencial en los medios no está cifrada, se debería considerar la protección física adicional de los medios.

9. CONTROL DE ACCESO

9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

9.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Guía de implementación

Los propietarios de los activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a sus activos, con la cantidad de detalle y severidad de los controles, que reflejen los riesgos de seguridad de la información asociados.

Los controles de acceso son tanto lógicos como físicos (véase el numeral 11) y se deberían considerar en conjunto. Se debería dar a los usuarios y a los proveedores de servicios una indicación clara de los requisitos del negocio que deben cumplir los controles de acceso.

La política debería tener en cuenta lo siguiente:

a) los requisitos de seguridad para las aplicaciones del negocio;

b) las políticas para la divulgación y autorización de la información, por ejemplo, el principio de lo que se necesita conocer, y los niveles de seguridad de la información y de clasificación de la información (véase el numeral 8.2);

c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes;

d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios (véase el numeral 18.1);

e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles;

f) la segregación de los roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso, administración del acceso;

g) los requisitos para la autorización formal de las solicitudes de acceso (véanse los numerales 9.2.1 y 9.2.2);

h) los requisitos para la revisión periódica de los derechos de acceso (véase el numeral 9.2.5);

i) el retiro de los derechos de acceso (véase el numeral 9.2.6);

j) el almacenamiento de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información secreta para la autenticación;

k) los roles de acceso privilegiado (véase el numeral 9.2.3);

Información adicional

Cuando se especifican las reglas de control de acceso se debería considerar:

a) establecer reglas basadas en la premisa “En general, todo está prohibido, a menos que se permita expresamente”, y no en la menos estricta: “En general, todo está permitido, a menos que se prohíba expresamente”;

b) los cambios en las etiquetas de información (véase el numeral 8.2.2) que son iniciados automáticamente por las instalaciones de procesamiento de información, y los que se inician a discreción del usuario.

c) los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información, y los iniciados por un administrador;

d) las reglas que requieren aprobación específica antes de su promulgación, y las que no requieren aprobación.

Las reglas de control de acceso deberían ir soportadas en procedimientos formales (véanse los numerales 9.2, 9.3, 9.4) y en responsabilidades definidas (véanse los numerales 6.1.1, y 9.3)

El control de acceso basado en roles es un enfoque usado con éxito por muchas organizaciones para establecer un vínculo entre los derechos de acceso y los roles del negocio.

Dos de los principios frecuentes que dirigen la política de control de acceso son:

a) lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber, y en consecuencia, diferentes perfiles de acceso);

b) lo que necesita usar: solamente se le concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

9.1.2 Acceso a redes y a servicios en red

Control

Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Guía de implementación

Se debería formular una política acerca del uso de redes y de servicios de red. Esta política debería cubrir:

a) las redes y servicios de red a los que se permite el acceso;

b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red;

c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red;

d) los medios usados para acceder a las redes y servicios de red (por ejemplo, el uso de VPN o redes inalámbricas);

e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red;

f) el monitoreo del uso de servicios de red.

La política sobre el uso de los servicios de red debería ser coherente con la política de control de acceso de la organización (véase el numeral 9.1.1).

Información adicional

Las conexiones no autorizadas y no seguras a los servicios de red pueden afectar a toda la organización. Este control es particularmente importante para conexiones de red o aplicaciones de negocios críticas o sensibles o para usuarios en sitios de alto riesgo, por ejemplo, áreas públicas o externas que se encuentran por fuera de la gestión y control de seguridad de la información de la organización.

9.2 GESTIÓN DE ACCESO DE USUARIOS

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

9.2.1 Registro y cancelación del registro de usuarios

Control

Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Guía de implementación

El proceso para gestionar la identificación de los usuarios debería incluir:

a) Usar identificaciones únicas que permitan asociar a los usuarios con sus actividades y hacerlos responsables de sus acciones; el uso de identificaciones compartidas solo se deberían permitir cuando sea necesario por razones operativas o del negocio, y se deberían aprobar y documentar;

b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización (véase el numeral 9.2.6);

c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes;

d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.

Información adicional

Suministrar o revocar el acceso a la información o a las instalaciones de procesamiento de información es habitualmente un procedimiento de dos pasos:

a) asignar y habilitar o revocar una identificación de usuario;

b) suministrar o revocar los derechos de acceso a esta identificación de usuario (véase el numeral 9.2.2).

9.2.2 Suministro de acceso de usuarios

Control

Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.

Guía de implementación

El proceso de suministro para asignar o revocar los derechos de acceso otorgados a las identificaciones de usuario debería incluir:

a) obtener autorización del propietario del sistema de información o servicio para el uso del sistema de información o servicio (véase el control 8.1.2); también puede ser apropiada la aprobación separada de los derechos de acceso por parte de la dirección;

b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso (véase el numeral 9.1) y es coherente con otros requisitos, tales como la segregación de funciones (véase el numeral 6.1.2);

c) asegurar que los derechos de acceso no estén activados (por ejemplo, por proveedores de servicio) antes de que los procedimientos de autorización estén completos;

d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios;

e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización;

f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios (véase el numeral 9.2.5).

Información adicional

Se debería considerar el establecimiento de los roles de acceso de usuarios con base en los requisitos del negocio que resumen varios derechos de acceso en perfiles típicos de acceso de usuario. Las solicitudes y revisiones de acceso (véase el numeral 9.2.4) se gestionan más fácilmente al nivel de estos roles que al nivel de derechos particulares.

Se debería considerar la inclusión, en los contractos del personal y en los contratos de servicio, numerales que especifiquen sanciones si miembros del personal o contratistas intentan acceso no autorizado (véanse los numerales 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Gestión de derechos de acceso privilegiado

Control

Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Guía de implementación:

La asignación de derechos de acceso privilegiado se debería controlar mediante un proceso de autorización formal de acuerdo con la política de control de acceso pertinente (véase el control 9.1.1). Se deberían considerar los siguientes pasos:

a) se deberían identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, por ejemplo, sistema operativo, sistema de gestión de bases de datos, y cada aplicación y los usuarios a los que es necesario asignar;

b) los derechos de acceso privilegiado se deberían asignar a usuarios con base en la necesidad de uso y caso por caso, en línea con la política de control de acceso (véase el numeral 9.1.1), es decir, con base en el requisito mínimo para sus roles funcionales;

c) se debería mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se deberían suministrar derechos de acceso cuando el proceso de autorización esté completo;

d) se deberían definir los requisitos para la expiración de los derechos de acceso privilegiado;

e) los derechos de acceso privilegiado se deberían asignar a una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se deberían ejecutar desde una identificación privilegiada;

f) las competencias de los usuarios con derechos de acceso privilegiado se deberían revisar con regularidad para verificar si están en línea con sus deberes;

g) se deberían establecer y mantener procedimientos específicos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema;

h) para las identificaciones de usuario de administración genérica, se debería mantener la confidencialidad de la información secreta para la autenticación cuando se comparta (por ejemplo, cambiar las contraseñas con frecuencia, y tan pronto como sea posible cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).

Información adicional

El uso inapropiado de los privilegios del sistema de administración (cualquier característica o función de un sistema de información que posibilita que el usuario anule el sistema o los controles de aplicación) es un factor que contribuye a las fallas o violaciones a los sistemas.

9.2.4 Gestión de información secreta para la autenticación de usuarios (*Management of Secret Authentication Information of Users*)

Control

La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.

Guía de implementación

Este proceso debería incluir los siguientes requisitos:

a) se debería pedir a los usuarios que firmen una declaración para mantener confidencial la información secreta para la autenticación personal, y mantener la información secreta para la autenticación del grupo (es decir, compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo (véase el numeral 7.1.2);

b) cuando se les pide a los usuarios mantener su propia información secreta para la autenticación, inicialmente se les debería suministrar información secreta y segura, que sea temporal para dicha autentificación, y se debería obligarles a cambiar dicha información, al usarla por primera vez;

c) se deberían establecer procedimientos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal;

d) la información secreta para la autenticación temporal se le debería suministrar a los usuarios de una manera segura; se debería evitar el uso de partes externas o de mensajes de correo electrónico no protegidos (texto claro);

e) la información secreta para la autenticación temporal debería ser única para un individuo y no debería ser fácil de adivinar;

f) los usuarios deberían acusar recibo de la información secreta para la autenticación;

g) la información secreta para la autenticación por defecto, del fabricante, se debería modificar después de la instalación de los sistemas o software.

Información adicional

Las contraseñas son un tipo de información secreta para la autenticación usadas comúnmente, y son un medio común para verificar la identidad del usuario. Otros tipos de información secreta para la autenticación son las llaves criptográficas y otros datos almacenados en *tokens* de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación.

9.2.5 Revisión de los derechos de acceso de usuarios

Control

Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

Guía de implementación

La revisión de los derechos de acceso debería considerar lo siguiente:

a) los derechos de acceso de los usuarios se deberían revisar a intervalos regulares y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo (véase el numeral 7);

b) los derechos de acceso de usuario se deberían revisar y reasignar cuando pasan de un rol a otro dentro de la misma organización;

c) las autorizaciones para los derechos de acceso privilegiado se deberían revisar a intervalos más frecuentes;

d) las asignaciones de privilegios se deberían verificar a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados;

e) los cambios a las cuentas privilegiadas se deberían registrar (*Logged*) para revisión periódica.

Información adicional

Este control compensa las posibles debilidades en la ejecución de los controles 9.2.1, 9.2.2 y 9.2.6.

9.2.6 Retiro o ajuste de los derechos de acceso

Control

Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.

Guía de implementación

Al terminar, los derechos de acceso de un individuo a información o a activos asociados con las instalaciones y servicios de procesamiento de la información se deberían retirar o suspender. Esto determinará si es necesario retirar los derechos de acceso. Los cambios de empleo se deberían reflejar en el retiro de todos los derechos de acceso que no fueron aprobados para el nuevo empleo. Los derechos de acceso que se deberían retirar o ajustar incluyen los de acceso físico y lógico. El retiro o ajuste se puede hacer mediante el retiro, revocación o reemplazo de llaves, tarjetas de identificación, instalaciones de procesamiento de información o suscripciones. Cualquier documentación que identifique los derechos de acceso de empleados y contratistas debería reflejar el retiro o ajuste de los derechos de acceso. Si un empleado o usuario de una parte externa que deja la empresa tiene contraseñas conocidas de usuarios que continúan activos, se deberían cambiar al terminar o cambiar de cargo o empleo, contrato o acuerdo.

Los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información se deberían reducir o retirar antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo tales como:

a) si la terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación;

b) las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario;

c) el valor de los activos accesibles en la actualidad.

Información adicional

En algunas circunstancias, los derechos de acceso se pueden asignar con base en la disponibilidad para más personas, además del empleado o el usuario de la parte externa que deja la organización, por ejemplo, identificaciones de grupo. En estas circunstancias, los individuos que dejan la organización se deberían retirar de cualquier lista de acceso de grupo, y se debería contar con disposiciones para advertir a todos los otros empleados y usuarios de partes externas involucrados, para que dejen de compartir esta información con estos individuos.

En los casos de terminación iniciada por la dirección, los empleados o usuarios de partes externas que se encuentren descontentos pueden corromper la información deliberadamente o sabotear las instalaciones de procesamiento de información. En el caso de personas que renuncian o que son despedidas, se pueden sentir tentadas a recolectar información para uso futuro.

9.3 RESPONSABILIDADES DE LOS USUARIOS

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

9.3.1 Uso de información secreta para la autenticación.

Control

Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información secreta para la autenticación.

Guía de implementación

Se debería notificar a todos los usuarios que:

a) Mantengan la confidencialidad de la información secreta para la autenticación, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad;

b) eviten llevar un registro (por ejemplo, en papel, en un archivo de software o en un dispositivo portátil) de la información secreta para la autenticación, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, una bóveda para contraseñas);

c) cambien la información secreta para la autenticación siempre que haya cualquier indicio de que se pueda comprometer la información;

d) cuando se usan contraseñas como información secreta para la autenticación, seleccione contraseñas de calidad con una longitud mínima suficiente que:

    1) sean fáciles de recordar;

    2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, por ejemplo, nombres, números de teléfono y fechas de nacimiento, etc.;

    3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios);

4) estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos;

5) si son temporales, cambiarlas la primera vez que se ingrese;

e) no compartan información secreta para la autenticación del usuario individual;

f) aseguren la protección apropiada de contraseñas cuando se usan éstas como Información secreta para la autenticación en procedimientos automatizados de ingreso (*Log-On*) y estén almacenadas

g) no usen la misma información secreta para la autenticación para propósitos de negocio y otros diferentes de éstos.

Información adicional

El suministro de un *Single Sign On* (SSO) u otras herramientas de gestión de información secreta para la autenticación reduce la cantidad de información secreta para la autenticación que los usuarios deben proteger, y de esta manera se incrementa la eficacia de este control. Sin embargo, estas herramientas también pueden incrementan el impacto de la divulgación de información secreta para la autenticación.

9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información

Control

El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

Guía de implementación

Las restricciones de acceso se deberían basar en los requisitos de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida.

Se debería considerar lo siguiente como soporte a los requisitos de restricción de acceso:

a) suministrar menús para controlar el acceso a la funcionalidad de las aplicaciones;

b) controlar a qué datos puede tener acceso un usuario particular;

c) controlar los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar;

d) controlar los derechos de acceso de otras aplicaciones;

e) limitar la información contenida en las salidas;

f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.

9.4.2 Procedimiento de ingreso (*Log-On*) seguro

Control

Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.

Guía de implementación

Se debería escoger una técnica de autenticación adecuada para corroborar la identidad declarada de un usuario.

En donde se requiere una verificación de la identidad y autenticación fuerte, se deberían usar métodos de autenticación alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, *tokens* o medios biométricos.

Se debería diseñar el procedimiento para ingresar (*Logging*) a un sistema o aplicación, para minimizar la oportunidad de acceso no autorizado. Por tanto, el procedimiento de ingreso (*Log-On*) debería divulgar la mínima información acerca del sistema o aplicación, con el fin de evitar que se suministre asistencia innecesaria a un usuario no autorizado.

Un procedimiento de ingreso (*Log-On*) adecuado debería:

a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso (*Log-On*) se haya completado exitosamente;

b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador;

c) evitar los mensajes de ayuda durante el procedimiento de ingreso (*log-on*), que ayudarían a un usuario no autorizado;

d) validar la información de ingreso (*Log-On*) solamente al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta;

e) proteger contra intentos de ingreso (*Log-On*) mediante fuerza bruta;

f) llevar un registro (*Log*) con los intentos exitosos y fallidos;

g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso (*Log-On*) seguro;

h) visualizar la siguiente información al terminar un ingreso (*log-on*) exitoso:

   1) la fecha y la hora del ingreso (*Log-On*) previo exitoso;

   2) los detalles de cualquier intento de ingreso (*Log-On*) no exitoso desde el último ingreso (*Log-On*) exitoso;

i) no visualizar una contraseña que se esté ingresando;

j) no transmitir contraseñas en texto claro en una red;

k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles;

l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

Información adicional

Las contraseñas son una forma común para brindar identificación y autenticación con base en un secreto que solamente conoce el usuario. Lo mismo se puede lograr con medios criptográficos y protocolos de autenticación. La fortaleza de la autenticación de usuario debería ser apropiada para la clasificación de la información a la que se va a acceder.

Si las contraseñas se transmiten en texto claro (*Clear Text*) durante la sesión de ingreso a la red, pueden ser capturadas por un programa *"sniffer*" "de redes.

9.4.3 Sistema de gestión de contraseñas

Control

Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

Guía de implementación

Un sistema de gestión de contraseñas debería:

a) hacer cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas;

b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada;

c) Exigir que se escojan contraseñas de calidad;

d) Forzar a los usuarios a cambiar sus contraseñas cuando ingresan por primera vez;

e) exigir que se cambien las contraseñas en forma regular, según sea necesario:

f) llevar un registro de las contraseñas usadas previamente, e impedir su reúso;

g) no visualizar contraseñas en la pantalla cuando se está ingresando;

h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicación (*Application System Data*);

i) almacenar y transmitir las contraseñas en forma protegida.

Información adicional

Algunas aplicaciones exigen que una autoridad independiente asigne las contraseñas de usuario; en estos casos, no se aplican los literales b), d) y e) anteriores. En la mayoría de casos, los usuarios son quienes seleccionan y mantienen las contraseñas.

9.4.4 Uso de programas utilitarios privilegiados

Control

Se debería restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Guía de implementación

Se deberían considerar las siguientes directrices para el uso de programas utilitarios que pudieran tener capacidad de anular los controles de sistemas y de aplicaciones.

a) el uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios;

b) la segregación de los programas utilitarios del software de aplicaciones;

c) la limitación del uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados (véase el numeral 9.2.3);

d) la autorización para el uso adhoc de programas utilitarios;

e) la limitación de la disponibilidad de los programas utilitarios, por ejemplo, para la duración de un cambio autorizado;

f) el registro (*logging*) de uso de los programas utilitarios;

g) la definición y documentación de los niveles de autorización para los programas utilitarios;

h) el retiro o deshabilitación de todos los programas utilitarios innecesarios;

No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas, en donde se requiera la segregación de funciones

Información adicional

La mayoría de instalaciones de cómputo tienen uno o más programas utilitarios que podrían tener capacidad para anular los controles de sistemas y aplicaciones.

9.4.5 Control de acceso a códigos fuente de programas

Control

Se debería restringir el acceso a los códigos fuente de los programas.

Guía de implementación

Se debería controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación), con el fin de evitar la introducción de funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.

Para los códigos fuente de los programas, esto se puede lograr mediante el almacenamiento central controlado de estos códigos, preferiblemente en librerías de fuentes de programas. Se deberían considerar las siguientes directrices para controlar el acceso a dichas librerías de fuentes de programa, para reducir el potencial de corrupción de los programas de computador:

a) Donde sea posible, las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción

b) la gestión de los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos;

c) el personal de soporte debería tener acceso restringido a las librerías de las fuentes de los programas;

d) la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se debería hacer una vez que se haya recibido autorización apropiada;

e) los listados de programas se deberían mantener en un entorno seguro;

f) se debería conservar un registro de auditoría (*Audit Log*) de todos los accesos a la librería de fuentes de programas;

g) el mantenimiento y copia de las librerías de fuentes de programas deberían estar sujetos a procedimientos estrictos de control de cambios (véase el numeral 14.2.2).

Si los códigos fuente de los programas están previstos para ser publicados, se deberían considerar controles adicionales para ayudar a asegurar su integridad (por ejemplo, firma digital).

10. CRIPTOGRAFÍA

10.1 CONTROLES CRIPTOGRÁFICOS

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

10.1.1 Política sobre el uso de controles criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Guía de implementación

Cuando se desarrolla una política sobre el uso de la criptografía, es conveniente tener en cuenta lo siguiente:

a) el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio;

b) con base en la valoración de riesgos, se debería identificar el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de cifrado requerido.

c) el uso de cifrado para la protección de información transportada por dispositivos móviles o removibles, o a través de líneas de comunicación;

d) el enfoque para la gestión de llaves, incluidos los métodos para la protección de llaves criptográficas y la recuperación de información cifrada , en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas;

e) roles y responsabilidades, por ejemplo, quién es responsable por:

   1) la implementación de la política.

   2) la gestión de llaves, incluida la generación de llaves (véase el numeral 10.1.2);

f) las normas que se van a adoptar para la implementación efectiva en toda la organización (qué solución se usa para los procesos del negocio);

g) el impacto de usar información cifrada en los controles que dependen de la inspección del contenido (por ejemplo, detección de software malicioso).

Cuando se implementa la política del uso de controles criptográficos de la organización, se deberían considerar las reglamentaciones y las restricciones nacionales que podrían aplicarse al uso de técnicas criptográficas en diferentes partes del mundo, y a las cuestiones de flujo de información cifrada entre fronteras, en diferentes partes del mundo (véase el numeral 18.1.5).

Los controles criptográficos se pueden usar para cumplir diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad; uso de información cifrada para proteger información sensible o crítica, ya sea almacenada o transmitida;

b) integridad/autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida;

c) no-repudio: uso de técnicas criptográficas para suministrar evidencia de que un evento o acción ocurre o no ocurre;

d) autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso a usuarios, entidades o recursos del sistema, o tener transacciones con ellos.

Información adicional

Tomar una decisión acerca de si una solución criptográfica es apropiada se debería considerar como parte de un proceso más amplio de valoración de riesgos y de selección de controles. Esta valoración se puede usar entonces para determinar si un control criptográfico es apropiado, qué tipo de control se debería aplicar y para qué propósito y procesos de negocio.

Es necesaria una política sobre el uso de controles criptográficos para maximizar los beneficios y minimizar los riesgos de usar técnicas criptográficas y para evitar el uso inapropiado o incorrecto.

Se debería buscar asesoría especializada para seleccionar controles criptográficos apropiados que cumplan los objetivos de la política de seguridad de la información.

10.1.2 Gestión de llaves

Control

Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

Guía de implementación

La política debería incluir requisitos para la gestión de llaves criptográficas durante todo su ciclo de vida, incluida la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las llaves.

Los algoritmos criptográficos, la longitud de las llaves y las prácticas de uso se deberían seleccionar de acuerdo con las mejores prácticas. Una gestión apropiada de las llaves requiere procesos seguros para la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de llaves criptográficas.

Todas las llaves criptográficas se deberían proteger contra modificación y pérdida. Además, las llaves secretas y privadas necesitan protección contra uso y divulgación no autorizados. Los equipos usados para generar, almacenar y archivar las llaves, deberían estar protegidos físicamente.

Un sistema de gestión de llaves debería estar basado en un grupo establecido de normas, procedimientos y métodos seguros para:

a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de llaves públicas;

c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves;

d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas;

e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deberían cambiar y cómo hacerlo;

f) dar tratamiento a las llaves cuya seguridad está comprometida;

g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización (en cuyo caso las llaves también se deberían archivar);

h) recuperar las llaves que estén perdidas o dañadas (*Corrupted*);

i) hacer copias de respaldo de las llaves o archivarlas;

j) destruir las llaves;

k) registrar (*Logging)* y auditar las actividades relacionadas con gestión de llaves.

Para reducir la posibilidad de uso inapropiado, se deberían definir fechas de activación y desactivación de las llaves, de manera que solo puedan usarse durante un periodo de tiempo definido en la política asociada de gestión de llaves.

Además de hacer la gestión segura de las llaves secretas y privadas, también se debería considerar la autenticidad de las llaves públicas. Este proceso de autenticación se puede hacer usando certificados de llaves públicas que normalmente expide una autoridad de certificación, que debería ser una organización reconocida con controles y procedimientos adecuados para suministrar el grado de confianza requerido.

El contenido de los acuerdos o contratos de nivel de servicio con los proveedores externos de servicios criptográficos, por ejemplo, con una autoridad de certificación, debería comprender cuestiones de responsabilidad civil, confiabilidad de los servicios y tiempos de respuesta para la prestación de los servicios (véase el numeral 15.2).

Información adicional

La gestión de las llaves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. La ISO/IEC 11770[2][3][4] brinda información sobre gestión de llaves.

Las técnicas criptográficas también se pueden usar para proteger las llaves criptográficas. Puede ser necesario considerar procedimientos para el manejo de solicitudes legales para acceder a las llaves criptográficas, por ejemplo, se puede requerir que la información cifrada se ponga a disposición en forma no cifrada, como evidencia en un juicio.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 ÁREAS SEGURAS

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

11.1.1 Perímetro de seguridad física

Control

Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.

Guía de implementación

Las siguientes directrices se deberían considerar e implementar cuando sea adecuado para los perímetros de seguridad física:

a) se deberían definir los perímetros de seguridad, y la ubicación y la fortaleza de cada uno de los perímetros deberían depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos;

b) los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información deberían ser físicamente seguros (es decir, no debería haber brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión ; el techo exterior, las paredes y los pisos del sitio deberían ser de construcción sólida, y todas las puertas externas deberían estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras); las puertas y ventanas deberían estar cerradas con llave cuando no hay supervisión, y se debería considerar protección externa para ventanas, particularmente al nivel del suelo;

c) debería haber un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debería estar restringido únicamente para personal autorizado;

d) en donde sea aplicable, se deberían construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental;

e) todas las puertas contra incendio en un perímetro de seguridad deberían tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deberían funcionar de manera segura de acuerdo al código local de incendios

f) se deberían instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deberían poner a prueba regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deberían tener alarmas en todo momento; también deberían abarcar otras áreas, tales como las salas de cómputo o las salas de comunicaciones;

g) las instalaciones de procesamiento de información gestionadas por la organización deberían estar separadas físicamente de las gestionadas por partes externas.

Información adicional

La protección física se puede lograr creando una o más barreras físicas alrededor de los predios y de las instalaciones de procesamiento de información de la organización. El uso de múltiples barreras brinda protección adicional, en donde la falla de una sola barrera no significa que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina que se pueda cerrar con llave, o varios recintos rodeados por una barrera de seguridad física interna. Se pueden necesitar perímetros y barreras adicionales para controlar el acceso físico entre las áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. Se debería prestar especial atención a la seguridad del acceso físico, en el caso de edificaciones que albergan activos para múltiples organizaciones.

La aplicación de los controles físicos, especialmente para las áreas seguras, se debería adaptar a las circunstancias técnicas y económicas de la organización, como se establece en la valoración de riesgos.

11.1.2 Controles de acceso físicos

Control

Las áreas seguras se deberían proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) se debería llevar un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deberían ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debería otorgar acceso para propósitos específicos autorizados y se deberían emitir instrucciones sobre los requisitos de seguridad del área y de los procedimientos de emergencia. La identidad de los visitantes se debería autenticar por los medios apropiados;

b) el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, por ejemplo, mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto;

c) se debería mantener y hacer seguimiento de un libro de registro (*Physical Log Book*) físico o un rastro de auditoría (*Audit Trail*) electrónica de todos los accesos;

d) todos los empleados, contratistas y partes externas deberían portar algún tipo de identificación visible, y se debería notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible;

e) al personal de servicio de soporte de una parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se debería autorizar y se le debería hacer seguimiento;

f) los derechos de acceso a áreas seguras se deberían revisar y actualizar regularmente, y revocar cuando sea necesario (véanse los numerales 9.2.5 y 9.2.6).

11.1.3 Seguridad de oficinas, recintos e instalaciones

Control

Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

Guía de implementación

Las siguientes directrices se deberían considerar para brindar seguridad a oficinas, recintos e instalaciones:

a) las instalaciones clave deberían estar ubicadas de manera que se impida el acceso del público;

b) en donde sea aplicable, las edificaciones deberían ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información;

c) las instalaciones deberían estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debería considerar apropiado;

d) los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deberían ser accesibles a ninguna persona no autorizada.

11.1.4 Protección contra amenazas externas y ambientales

Control

Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Guía de implementación

Se debería obtener asesoría especializada acerca de cómo evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

11.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) el personal solo debería conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer;

b) el trabajo no supervisado en áreas seguras se debería evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas;

c) las áreas seguras vacías deberían estar cerradas con llave y se deberían revisar periódicamente;

d) no se debería permitir equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

Las disposiciones para trabajo en áreas seguras incluyen controles para los empleados y usuarios de partes externas que trabajan en el área segura, y cubren todas las actividades que ocurren en el área segura.

11.1.6 Áreas de despacho y carga

Control

Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado;

b) el área de despacho y carga se debería diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación;

c) las puertas externas de un área de despacho y carga se deberían asegurar cuando las puertas internas están abiertas;

d) el material que ingresa se debería inspeccionar y examinar para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga;

e) el material que ingresa se debería registrar de acuerdo con los procedimientos de gestión de activos (véase el numeral 8) al entrar al sitio;

f) los despachos entrantes y salientes se deberían separar físicamente, en donde sea posible;

g) el material entrante se debería inspeccionar para determinar evidencia de alteración durante el viaje. Si se descubre tal alteración, se debería reportar de inmediato al personal de seguridad.

11.2 EQUIPOS

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

11.2.1 Ubicación y protección de los equipos

Control

Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

Guía de implementación

Se deberían considerar las siguientes directrices para proteger los equipos:

a) los equipos se deberían ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;

b) las instalaciones de procesamiento de la información que manejan datos sensibles deberían estar ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso;

c) las instalaciones de almacenamiento se deberían asegurar para evitar el acceso no autorizado;

d) los elementos que requieren protección especial se deberían salvaguardar para reducir el nivel general de protección requerida;

e) se deberían adoptar controles para minimizar el riesgo de amenazas físicas y ambientales potenciales, por ejemplo, robo, incendio, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

f) se deberían establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información;

g) se debería hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información;

h) la protección contra descargas eléctricas atmosféricas se debería aplicar a todas las edificaciones y se deberían colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas;

i) se debería considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales;

j) los equipos para procesamiento de información confidencial se deberían proteger para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.

11.2.2 Servicios de suministro

Control

Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

Guía de implementación

Los servicios de suministro (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) deberían:

a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales;

b) evaluarse regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte;

c) inspeccionarse y probarse regularmente para asegurar su funcionamiento apropiado;

d) si es necesario, contar con alarmas para detectar mal funcionamiento;

e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.

Se debería suministrar iluminación y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para interrumpir la energía, el agua, el gas u otros servicios deberían estar localizados cerca de las salidas de emergencia o recintos de equipos.

Información adicional

Se puede obtener redundancia adicional para conectividad de redes por medio de múltiples rutas desde uno o más proveedores de servicios.

11.2.3 Seguridad del cableado

Control

El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño.

Guía de implementación

Se deberían considerar las siguientes directrices para seguridad del cableado:

a) las líneas de energía eléctrica y de telecomunicaciones que entran a instalaciones de procesamiento de información deberían ser subterráneas en donde sea posible, o deberían contar con una protección alternativa adecuada;

b) los cables de energía eléctrica deberían estar separados de los cables de comunicaciones para evitar interferencia;

c) para sistemas sensibles o críticos los controles adicionales que se debería considerar incluyen:

   1) la instalación de tuberías blindadas y recintos o cajas con llave en los puntos de inspección y de terminación;

   2) el uso de blindaje electromagnético para proteger los cables;

   3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables;

   4) el acceso controlado a los paneles de conexión y recintos de cables.

11.2.4 Mantenimiento de equipos

Control

Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

Guía de implementación

Se deberían considerar las siguientes directrices para mantenimiento de equipos:

a) los equipos se deberían mantener de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor;

b) solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos;

c) se deberían llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo;

d) se deberían implementar controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debería remover (*Cleared*) del equipo, o el personal de mantenimiento debería ser suficientemente revisado (*Cleared*);

e) se deberían cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros (*Insurance Policies*);

f) antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para *asegurarse* de que no ha sido alterado y que su funcionamiento es adecuado.

11.2.5 Retiro de activos

Control

Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.

Guía de implementación

Se deberían considerar las siguientes directrices:

a) se deberían identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio;

b) se deberían establecer los límites de tiempo para el retiro de activos y se debería verificar que se cumplen las devoluciones;

c) cuando sea necesario y apropiado, se debería registrar cuando los activos se retiran del sitio y cuando se hace su devolución;

d) se debería documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software.

Información adicional

Los chequeos puntuales (*Spot Check*), que se realizan para detectar el retiro no autorizado de activos, también se pueden llevar a cabo para detectar dispositivos de registro no autorizados, armas, etc., y para impedir su entrada y salida del sitio. Estos chequeos puntuales (*Spot Check*) se deberían llevar a cabo de acuerdo con la legislación y reglamentaciones pertinentes. Se debería informar a los individuos que se realizan chequeos puntuales (*Spot Check*), y las verificaciones se deberían llevar a cabo solo con la autorización apropiada para los requisitos legales y de reglamentación.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Control

Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

Guía de implementación

El uso de cualquier equipo de almacenamiento y procesamiento de información por fuera de las instalaciones de la organización debería ser aprobado por la dirección. Esto se aplica a equipos de propiedad de la organización y a equipos de propiedad privada y usados a nombre de la organización.

Se deberían considerar las siguientes directrices para proteger los equipos fuera de las instalaciones:

a) los equipos y medios retirados de las instalaciones no se deberían dejar sin vigilancia en lugares públicos;

b) en todo momento se deberían seguir las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposición a campos electromagnéticos fuertes;

c) los controles para lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deberían determinar mediante una valoración de riesgos y se deberían aplicar los controles adecuados según sean apropiados, por ejemplo, gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina (véase también la norma ISO/IEC 27033 [15][16][17][18][19]);

d) cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos o partes externas, se debería llevar un registro (*log*) que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.

Los riesgos, por ejemplo, de daño, robo o interceptación de conversaciones pueden variar considerablemente entre ubicaciones, y se deberían tener en cuenta al determinar los controles más apropiados.

Información adicional

El equipo de procesamiento y almacenamiento de información incluye todas las formas de computadores personales, organizadores, teléfonos móviles, tarjetas inteligentes, papel u otro formato, que se mantenga para trabajo en la casa o que se transporte lejos del lugar de trabajo normal.

En el numeral 6.2 se puede encontrar más información acerca de otros aspectos de la protección de equipos móviles.

Puede ser apropiado evitar el riesgo, desalentando a algunos empleados para que no trabajen fuera del sitio, o restringiendo el uso de equipos de TI portátiles;

11.2.7 Disposición segura o reutilización de equipos

Control

Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.

Guía de implementación

Antes de la disposición o reúso de los equipos, se debería verificar que estos no contengan medios de almacenamiento.

Los medios de almacenamiento que contienen información confidencial o protegida por derechos de autor se deberían destruir físicamente, o la información debería ser destruida, eliminada o sobrescrita usando técnicas para hacer que la información original no sea recuperable, en vez de usar la función estándar borrar o formatear.

Información adicional

Los equipos dañados que contienen medios de almacenamiento pueden requerir una valoración de riesgos para determinar si los elementos se deberían destruir físicamente en vez de enviarlos a reparar o desechar. La información se puede comprometer debido a una disposición descuidada o reúso de equipos.

Además de asegurar el borrado de discos, el cifrado del disco entero reduce el riesgo de que se divulgue información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando:

a) el proceso de cifrado sea suficientemente fuerte y abarque el disco (incluido el espacio libre (*Slack Space*), archivos de intercambio (*Swap File*), etc.);

b) las llaves criptográficas sean lo suficientemente largas para resistir ataques de fuerza bruta;

c) las llaves criptográficas se mantengan confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para asesoría adicional sobre criptografía, véase el numeral 10.

Las técnicas para sobreescribir en forma segura medios de almacenamiento son diferentes de acuerdo con la tecnología del medio de almacenamiento. Las herramientas de sobreescritura se deberían revisar para asegurarse de que son aplicables a la tecnología de los medios de almacenamiento.

11.2.8 Equipos de usuario desatendidos

Control

Los usuarios deberían asegurarse de que a los equipos desatendidos se les da protección apropiada.

Guía de implementación

Todos los usuarios deberían tomar conciencia de los requisitos y procedimientos de seguridad para proteger los equipos desatendidos, al igual que sus responsabilidades para la implementación de esta protección. Se debería notificar a los usuarios que:

a) terminen las sesiones activas cuando hayan finalizado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado, por ejemplo, un protector de pantalla protegido con contraseña;

b) cierren (*Log-Off*) las aplicaciones o servicios de red cuando ya no los necesiten;

c) aseguren los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente, por ejemplo, acceso con contraseña, cuando no están en uso.

11.2.9 Política de escritorio limpio y pantalla limpia

Control

Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

Guía de implementación

La política de escritorio limpio y de pantalla limpia debería tener en cuenta las clasificaciones de información (véase el numeral 8.2), los requisitos legales y contractuales (véase el numeral 18.1) y los riesgos y aspectos culturales correspondientes de la organización. Se deberían considerar las siguientes directrices:

a) la información sensible o crítica del negocio, por ejemplo, sobre papel o en un medio de almacenamiento electrónico, se debería guardar (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada.

b) cuando están desatendidos, los computadores y terminales se deberían dejar fuera del sistema (*Logged Off*) o proteger con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, *token* o mecanismo similar de autenticación de usuario, y deberían estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso;

c) se debería evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales);

d) los medios que contienen información sensible o clasificada se deberían retirar de las impresoras inmediatamente.

Información adicional

Una política de escritorio limpio / pantalla limpia reduce los riesgos de acceso no autorizado, pérdida y daño de información durante y por fuera de las horas laborales normales. Las cajas fuertes u otras formas de instalaciones de almacenamiento seguro podrían proteger la información almacenada en ellas contra desastres tales como incendios, terremotos, inundaciones o explosión.

Considere el uso de impresoras con función de código con PIN, de manera que los originadores sean los únicos que pueden hacer impresiones y solo cuando están al lado de la impresora.

12. SEGURIDAD DE LAS OPERACIONES

12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos de operación documentados

Control

Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesitan.

Guía de implementación

Se deberían preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación, tales como los procedimientos de encendido y apagado, copias de respaldo, mantenimiento de equipos, manejo de medios, salas de cómputo y gestión y seguridad del manejo de correo.

Los procedimientos de operación deberían especificar las instrucciones operacionales, que incluyen:

a) la instalación y configuración de sistemas;

b) el procesamiento y manejo de información, tanto automático como manual;

c) las copias de respaldo (véase el numeral 12.3);

d) los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos;

e) las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de utilidades del sistema (véase el numeral 9.4.4);

f) contactos de apoyo y de una instancia superior (escalamiento), incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas;

g) instrucciones sobre manejo de medios y elementos de salida especiales, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos (véanse los numerales 8.3 y 11.2.7);

h) procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema;

i) la gestión de rastros de auditoría (*Audit Trail*) y de la información de registro del sistema (*System Log*) (véase el numeral 12.4);

j) procedimientos de seguimiento.

Los procedimientos de operación y los procedimientos documentados para actividades del sistema se deberían tratar como documentos formales y cambios autorizados por la dirección. En donde sea viable técnicamente, la gestión de los sistemas de información se debería hacer de forma coherente, usando los mismos procedimientos, herramientas y utilitarios.

12.1.2 Gestión de cambios

Control

Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Guía de implementación

En particular, se deberían considerar los siguientes asuntos:

a) la identificación y registro de cambios significativos;

b) la planificación y puesta a prueba de los cambios;

c) la valoración de los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información;

d) el procedimiento de aprobación formal para los cambios propuestos;

e) la verificación de que se han cumplido los requisitos de seguridad de la información;

f) la comunicación de todos los detalles de los cambios a todas las personas pertinentes;

g) los procedimientos de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos;

h) el suministro de un proceso de cambio de emergencia que permita la implementación rápida y controlada de los cambios necesarios para resolver un incidente (véase el numeral 16.1).

Deberían existir responsabilidades y procedimientos de gestión formales para asegurar el control satisfactorio de todos los cambios. Cuando se hacen los cambios, se debería conservar un registro de auditoría (*Audit Log*) que contenga toda la información pertinente.

Información adicional

El control inadecuado de los cambios en las instalaciones y sistemas de procesamiento de la información es una causa común de fallas en el sistema o en la seguridad. Los cambios en el ambiente de producción, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la de producción, puede tener impacto sobre la confiabilidad de las aplicaciones (véase el numeral 14.2.2).

12.1.3 Gestión de capacidad

Control

Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

Guía de implementación

Los requisitos de capacidad se deberían identificar teniendo en cuenta la criticidad que tiene para el negocio el sistema involucrado. Se deberían aplicar el ajuste y seguimiento del sistema, para asegurar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Se deberían aplicar controles de detección que indiquen los problemas oportunamente. Las proyecciones de los requisitos sobre la capacidad futura deberían tener en cuenta los requisitos de los nuevos negocios y sistemas, y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.

Es necesario prestar atención particular a cualquier recurso con tiempos prolongados de espera para su adquisición, o costos altos; por tanto, los gerentes deberían hacer seguimiento de la utilización de los recursos clave del sistema; Deberían identificar tendencias en el uso, particularmente en relación con aplicaciones del negocio o herramientas de gestión de sistemas de la información.

Los gerentes deberían usar esta información para identificar y evitar cuellos de botella potenciales y dependencia del personal clave, que podrían presentar una amenaza para la seguridad o servicios del sistema, y planificar la acción apropiada.

Se puede suministrar capacidad suficiente incrementando la capacidad o reduciendo la demanda. Algunos ejemplos de gestión de la demanda de capacidad incluyen:

a) eliminación de datos obsoletos (espacio en disco);

b) el cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes;

c) la optimización de cronogramas y procesamiento de lotes;

d) la optimización de las consultas de bases de datos o lógicas de las aplicaciones;

e) la negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).

Se debería considerar un plan de gestión de capacidad documentado para sistemas críticos de la misión.

Información adicional

Este control también tiene en cuenta la capacidad de los recursos humanos, al igual que las oficinas e instalaciones.

12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Control

Se deberían separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

Guía de implementación

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

Se deberían considerar los siguientes asuntos:

a) se deberían definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de producción.

b) el software de desarrollo y de producción debería funcionar en diferentes sistemas o procesadores de cómputo y en diferentes dominios o directorios;

c) los cambios en los sistemas de producción y aplicaciones se deberían poner a prueba en un ambiente de pruebas antes de aplicarlos a los sistemas en producción.;

d) solo en circunstancias excepcionales, las pruebas no se deberían llevar a cabo en los sistemas en producción;

e) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema (*System Utilities*) no deberían ser accesibles desde sistemas en producción cuando no se requiere;

f) los usuarios deberían usar diferentes perfiles para sistemas en producción y de pruebas, y los menús deberían desplegar mensajes de identificación apropiados para reducir el riesgo de error;

g) los datos sensibles no se deberían copiar en el ambiente de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas (véase el numeral 14.3).

Información adicional

Las actividades de desarrollo y de pruebas pueden causar problemas graves, por ejemplo, la modificación involuntaria de archivos o del ambiente del sistema o falla del sistema. Es necesario mantener un ambiente conocido y estable en el cual se realicen pruebas significativas, e impedir el acceso de un desarrollador inapropiado, al ambiente de producción.

En donde el personal de desarrollo y pruebas tiene acceso al sistema en producción y a su información, puede estar en capacidad de introducir códigos no autorizados y no probados, o de alterar los datos de producción. En algunos sistemas, esta capacidad se puede utilizar indebidamente para cometer fraude o para introducir códigos no probados o maliciosos, que pueden causar serios problemas de operación.

El personal de desarrollo y pruebas también representa una amenaza a la confidencialidad de la información operacional. Las actividades de desarrollo y de pruebas pueden causar cambios imprevistos en el software o en la información, si comparten el mismo ambiente de cómputo. Por tanto, es recomendable separar los ambientes de desarrollo, prueba y producción, para reducir el riesgo de cambio accidental o acceso no autorizado al software operacional y a datos del negocio (véase el numeral 14.3 para la protección de los datos de prueba).

12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

12.2.1 Controles contra códigos maliciosos

Control

Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Guía de implementación

La protección contra los códigos maliciosos se debería basar en software de detección de códigos maliciosos y de reparación, en toma de conciencia sobre la seguridad de la información, y en controles apropiados de gestión de cambios y de acceso al sistema. Se deberían considerar las siguientes directrices:

a) establecer una política formal que prohíba el uso de software no autorizado (véanse los numerales 12.6.2 y 14.2.);

b) implementar controles para evitar o detectar el uso de software no autorizado (por ejemplo, listas blancas de aplicaciones);

c) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (por ejemplo, listas negras);

d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deberían tomar;

e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, por ejemplo, por medio de la gestión de la vulnerabilidad técnica (véase el numeral 12.6);

f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas;

g) la instalación y actualización regular del software de detección y reparación del software malicioso para analizar los computadores y medios como una medida de control o en forma rutinaria; el análisis realizado debería incluir:

   1) el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso;

   2) el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, por ejemplo, en los servidores de los correos electrónicos, en los computadores de escritorio y cuando se ingresa a la red de la organización;

   3) el análisis de páginas web, para determinar el software malicioso;

h) la definición de procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso;

i) la preparación de planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación (véase el numeral 12.3);

j) la implementación de procedimientos para recolectar información en forma regular, como por ejemplo la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso;

k) la implementación de procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos; los gerentes se deberían asegurar de que se usan fuentes calificadas, por ejemplo, publicaciones respetables, sitios o proveedores en Internet confiables que producen software de protección contra software malicioso, para diferenciar entre falsas alarmas (*Hoaxes*) y software malicioso real; todos los usuarios deberían tomar conciencia del problema de las falsas alarmas (*Hoaxes*) y de qué hacer en caso de recibirlas;

l) el aislamiento de ambientes en donde se pueden obtener impactos catastróficos.

Información adicional

El uso de dos o más productos de software que protegen contra software malicioso a través del ambiente de procesamiento de información, de diferentes vendedores y tecnología pueden mejorar la eficacia de la protección contra el software malicioso.

Es necesario protegerse contra la introducción de software malicioso durante los procesos de mantenimiento y de emergencia, el cual puede evitar los controles normales de protección contra software malicioso.

Bajo condiciones determinadas, la protección contra software malicioso podría causar perturbaciones dentro de las operaciones.

Habitualmente no es adecuado el uso por sí solo de software de detección y reparación de software malicioso, y comúnmente necesita estar acompañado de procedimientos de operación que impiden la introducción de software malicioso.

12.3 COPIAS DE RESPALDO

Objetivo: Proteger contra la pérdida de datos.

12.3.1 Respaldo de la información

Control

Se deberían hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Guía de implementación

Se debería establecer una política de copias de respaldo para definir los requisitos de la organización para copias de respaldo de información, software y sistemas.

La política de copias de respaldo debería definir los requisitos de retención y de protección.

Se deberían proporcionar instalaciones adecuadas para copias de respaldo, para asegurar que la información y el software esenciales se puedan recuperar después de un desastre o falla del medio.

Cuando se diseña un plan de copias de respaldo, se deberían tener en cuenta los siguientes aspectos:

a) se deberían producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados;

b) el alcance (por ejemplo, copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo deberían reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización;

c) las copias de respaldo se deberían almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal;

d) a la información de respaldo se le debería dar un nivel apropiado de protección física y del entorno (véase el numeral 11), de coherencia con las normas aplicadas en el sitio principal;

e) los medios de respaldo se deberían poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debería verificar contra el tiempo de restauración requerido. La prueba de la capacidad para restaurar datos de los que se ha hecho una copia de respaldo se debería hacer en medios de prueba dedicados, no sobreescribiendo el medio original, en caso de que el proceso de elaboración de copias de respaldo o de restauración falle y cause daño o pérdida de datos irreparable;

f) en situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deberían estar protegidas por medio de cifrado.

Los procedimientos de operación deberían monitorear la ejecución de las copias de respaldo y darle tratamiento a las fallas de las copias de respaldo programadas, para asegurar que se realiza de manera completa y de acuerdo con las políticas de copias establecidas para las mismas.

Las disposiciones relativas a copias de respaldo para sistemas y servicios individuales se deberían probar con regularidad para asegurar que cumplan los requisitos de los planes de continuidad de negocio. En el caso de sistemas y servicios críticos, las disposiciones relativas a copias de respaldo deberían abarcar toda la información de sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en caso de desastre.

Se debería determinar el período de retención de la información esencial del negocio, teniendo en cuenta cualquier requisito para copias de archivo que se van a retener permanentemente.

12.4 REGISTRO (*LOGGING*) Y SEGUIMIENTO

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de eventos

Control

Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Guía de implementación

Los registros de eventos (*Event Logs*) deberían incluir, cuando es pertinente:

a) identificación de usuarios;

b) actividades del sistema;

c) fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;

d) identidad del dispositivo o ubicación, si es posible, e identificador del sistema;

e) registros de intentos de acceso al sistema exitosos y rechazados;

e) registros de datos exitosos y rechazados y otros intentos de acceso a recursos;

g) cambios a la configuración del sistema;

h) uso de privilegios;

i) uso de utilidades y aplicaciones del sistema;

j) archivos a los que se tuvo acceso, y el tipo de acceso;

k) direcciones y protocolos de red;

l) alarmas accionadas por el sistema de control de acceso;

m) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;

n) registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

El registro de eventos (*Events Logging*) establece las bases para los sistemas de seguimiento automatizados que están en capacidad de generar informes consolidados y alertas sobre la seguridad del sistema.

Información adicional

Los registros de eventos (*Event Logs*) pueden contener datos sensibles e información identificable personalmente. Se deberían tomar medidas apropiadas para la protección de la privacidad (véase el numeral 18.1.4).

En donde sea posible, los administradores de sistemas no deberían tener permiso para borrar o desactivar registros (*Logs)* de sus propias actividades (véase el numeral 12.4.3).

12.4.2 Protección de la información de registro (*log information*)

Control

Los sistemas de gestión de registros (*Logging Facilities*) y la información de registro (*Log Information*) se deberían proteger contra alteración y acceso no autorizado.

Guía de implementación

Los controles deberían estar dirigidos a proteger contra cambios no autorizados de la información del registro (*Log Information*) y contra problemas operacionales con los sistemas de gestión de registros (*logging facilities*), inclusive:

a) alteraciones a los tipos de mensaje que se registran;

b) archivos de registro (*Log Files*) que son editados o eliminados;

c) se excede la capacidad de almacenamiento del medio de archivo de registro (*Log File Media*), lo que da como resultado falla en el registro de eventos, o sobreescritura de eventos pasados registrados.

Puede ser necesario archivar algunos registros de auditoría (*Audit Log*), como parte de la política de retención de registros o debido a requisitos acerca de recolectar y retener evidencia (véase el numeral 16.1.7).

Información adicional

Los registros del sistema (*System Logs*) a menudo contienen un gran volumen de información, mucha de la cual es ajena al seguimiento de la seguridad de la información. Para ayudar a identificar los eventos significativos con propósitos de seguimiento de la seguridad de la información, se debería considerar el copiado automático de tipos de mensajes apropiados a un segundo registro (*log*), o el uso de utilidades del sistema (*System Utilities*) o herramientas de auditoría adecuados para llevar a cabo la interrogación y racionalización de los archivos.

Es necesario proteger los registros del sistema (*System Logs*), ya que si los datos se pueden modificar o los datos en ellos se pueden borrar, su existencia puede crear una sensación falsa de seguridad. El copiado de registros (*Logs*) en tiempo real a un sistema por fuera del control de un administrador u operador del sistema se puede usar para salvaguardar los registros (*Logs*).

12.4.3 Registros (*Logs*) del administrador y del operador

Control

Las actividades del administrador y del operador del sistema se deberían registrar (*Logged*), y los registros (*Log*s) se deberían proteger y revisar con regularidad.

Guía de implementación

Los titulares de cuenta de usuario privilegiado pueden estar en capacidad de manipular los registros (*Logs*) en instalaciones de procesamiento de información bajo su control directo; por esto, es necesario proteger y revisar los registros (*Logs*) para mantener la rendición de cuentas para los usuarios privilegiados.

Información adicional

Un sistema de detección de intrusión gestionado por fuera del control del sistema y de los administradores de la red se puede usar para hacer seguimiento del sistema y de las actividades de administración de la red, para determinar su cumplimiento.

12.4.4 Sincronización de relojes

Control

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

Guía de implementación

Se deberían documentar los requisitos externos e internos para la representación de tiempo, sincronización y exactitud. Estos requisitos pueden ser legales, de reglamentación, contractuales, de cumplimiento con normas o requisitos para seguimiento interno. Se debería definir un tiempo de referencia estándar para uso dentro de la organización.

Se debería documentar e implementar el enfoque de la organización para obtener un tiempo de referencia de una(s) fuente(s) externas y como sincronizar confiablemente los relojes internos.

Información adicional

El ajuste correcto de los relojes de computador es importante para asegurar la exactitud de los registros de auditoría (*Audit Logs*), que pueden ser necesarios para investigaciones o como evidencia legal en casos legales o casos disciplinarios. Los registros de auditoría (*Audit Logs*) inexactos pueden dificultar estas investigaciones y afectar la credibilidad de esta evidencia. Un reloj vinculado a una transmisión de tiempo por radio desde un reloj atómico nacional se puede usar como el reloj maestro para los sistemas de registro (*Logging Systems*). Se puede usar un protocolo de tiempo de red para mantener todos los servidores sincronizados con el reloj maestro.

12.5 CONTROL DE SOFTWARE OPERACIONAL

Objetivo: Asegurar la integridad de los sistemas operativos (*Operational Systems*)

12.5.1 Instalación de software en sistemas operativos (*Operational Systems*)

Control

Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos (*Operational Systems*).

Guía de implementación

Se deberían considerar las siguientes directrices para controlar los cambios de software en sistemas operativos:

a) la actualización del software operacional, aplicaciones y librerías de programas solo la deberían llevar a cabo administradores entrenados, con autorización apropiada de la dirección (véase el numeral 9.4.5);

b) los sistemas operativos sólo deberían contener códigos ejecutables aprobados, no el código de desarrollo o compiladores;

c) las aplicaciones y el software del sistema operativo solo se deberían implementar después de pruebas extensas y exitosas; los ensayos deberían abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se deberían llevar a cabo en sistemas separados (véase el numeral 12.1.4); se debería asegurar que todas las librerías de fuentes de programas correspondientes hayan sido actualizadas;

d) se debería usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema;

e) se debería establecer una estrategia de retroceso (*Rollback*) antes de implementar los cambios;

f) se debería mantener un registro de auditoría (*Audit Log*) de todas las actualizaciones de las librerías de programas operacionales;

g) las versiones anteriores del software de aplicación se deberían conservar como una medida de contingencia;

h) las versiones de software anteriores se deberían archivar, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo.

El software suministrado por el vendedor, usado en los sistemas operacionales, se debería mantener a un nivel apoyado por el proveedor. Con el tiempo, los fabricantes de software dejarán de brindar soporte a las versiones de software anteriores. La organización debería considerar los riesgos de depender de software sin soporte.

Cualquier decisión de actualizarse a una nueva versión debería tener en cuenta los requisitos del negocio para el cambio y la seguridad de la versión, por ejemplo, la introducción de una nueva funcionalidad de seguridad de la información, o el número y severidad de los problemas de seguridad de la información que afectan a esta versión. Se deberían aplicar parches de software cuando pueden ayudar a eliminar o reducir debilidades de seguridad de la información (véase el numeral 12.6).

Sólo se debería conceder acceso lógico y físico a los proveedores para propósitos de apoyo cuando es necesario, y con aprobación de la dirección. Se debería hacer seguimiento a las actividades de los proveedores (véase el numeral 15.2.1).

El software informático puede depender de software y módulos suministrados externamente, a lo cual se debería hacer seguimiento y se debería controlar para evitar cambios no autorizados que puedan introducir debilidades en la seguridad.

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas

Control

Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Guía de implementación

Un inventario actualizado y completo de los activos (véase el numeral 8) es un prerrequisito para una gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, los números de las versiones, el estado actual de despliegue (por ejemplo, qué software se instaló en qué sistemas), y la(s) persona(s) dentro de la organización responsables por el software.

Se deberían tomar acciones apropiadas y oportunas en respuesta a la identificación de vulnerabilidades técnicas potenciales. Los siguientes aspectos se deberían seguir para establecer un proceso de gestión eficaz para las vulnerabilidades técnicas:

a) la organización debería definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;

b) los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se deberían identificar para el software y otra tecnología (con base en la lista de inventario de activos, véase 8.1.1); estos recursos de información se deberían actualizar con base en los cambios en el inventario o cuando se encuentran otros recursos nuevos o útiles;

c) se debería definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente;

d) una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles;

e) dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios (véase el numeral 12.1.2), o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (véase el numeral 16.1.5);

f) si está disponible un parche de una fuente legítima, se deberían valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se deberían comparar con el riesgo de instalar el parche);

g) los parches se deberían probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se deberían considerar otros controles como:

    1) dejar de operar (*Turning Off*) los servicios o capacidades relacionados con la vulnerabililidad;

2) adaptar o adicionar controles de acceso, por ejemplo, firewalls, en los límites de la red (véase el numeral 13.1);

3) incrementar el seguimiento para detectar ataques reales;

4) hacer tomar conciencia sobre la vulnerabilidad;

h) se debería llevar un registro de auditoría (*Audit Log*) para todos los procedimientos realizados;

i) se debería hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia;

j) se deberían abordar primero los sistemas que están en alto riesgo;

k) un proceso de gestión eficaz de la vulnerabilidad técnica debería estar alineado con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente;

l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.

Información adicional

La gestión de la vulnerabilidad técnica se puede considerar como una subfunción de la gestión de cambios, y como tal puede tomar ventaja de los procesos y procedimientos de gestión del cambio (véanse los numerales 12.1.2 y 14.2.2).

Con frecuencia, los vendedores experimentan una presión significativa para que liberen los parches lo más pronto posible. Por tanto, existe una posibilidad de que un parche no aborde el problema adecuadamente, y que tenga efectos negativos. Además, en algunos casos no es fácil desinstalar un parche una vez que se ha aplicado.

Si no es posible hacer una prueba adecuada de los parches, por ejemplo, debido a los costos o a la falta de recursos, se puede considerar un retraso en la colocación del parche para evaluar los riesgos asociados con base en la experiencia reportada por otros usuarios. El uso de la norma ISO/IEC 27031[14] puede ser beneficioso.

12.6.2 Restricciones sobre la instalación de software

Control

Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

Guía de implementación

La organización debería definir una política estricta, y hacerla cumplir, con relación a qué tipo de software pueden instalar los usuarios.

Se debería aplicar el principio del menor privilegio. Si se les han otorgado algunos privilegios, los usuarios pueden tener la capacidad de instalar software. La organización debería identificar qué tipos de instalaciones de software se permiten (por ejemplo, actualizaciones y parches de seguridad al software existente) y qué tipo de instalaciones están prohibidas (por ejemplo, que sea solamente para uso personal cuya idoneidad con relación a que sea potencialmente malicioso se conoce o se sospecha). Estos privilegios se deberían conceder con relación a los roles de los usuarios involucrados.

Información adicional

La instalación no controlada de software en dispositivos de computo puede conducir a que se introduzcan vulnerabilidades y posteriormente a fuga de información, pérdida de integridad u otros incidentes de seguridad de la información, o a la violación de derechos de propiedad intelectual.

12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos (*Operational Systems*).

12.7.1 Controles sobre auditorías de sistemas de información

Control

Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Guía de implementación

Se deberían observar las siguientes directrices:

a) los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con la dirección apropiada;

b) el alcance de las pruebas técnicas de auditoría se debería acordar y controlar;

c) las pruebas de auditoría se deberían limitar a acceso a software y datos únicamente para lectura;

d) el acceso diferente al de solo lectura solamente se debería prever para copias aisladas de los archivos del sistema (*System Files*), que se deberían borrar una vez que la auditoría haya finalizado, o se debería proporcionar protección apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría;

e) los requisitos para procesos especiales o adicionales se deberían identificar y acordar;

f) las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deberían realizar fuera de horas laborales;

g) se debería hacer seguimiento de todos los accesos y regístralos (*Logged*) para producir un rastro de referencia (*Reference Trail)*.

13. SEGURIDAD DE LAS COMUNICACIONES

13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

13.1.1 Controles de redes

Control

Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

Guía de implementación

Se deberían implementar controles para asegurar la seguridad de la información en las redes, y la protección de servicios relacionados, contra acceso no autorizado. En particular, se deberían considerar los siguientes elementos:

a) se deberían establecer las responsabilidades y procedimientos para la gestión de equipos de redes;

b) la responsabilidad operacional por las redes se debería separar de las operaciones de computo, en donde sea apropiado (véase el numeral 6.1.2);

c) se deberían establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados (véanse los numerales 10 y 13.2); también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados;

d) se deberían aplicar el registro (*Logging)* y el seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información;

e) las actividades de gestión se deberían coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información;

f) los sistemas en la red se deberían autenticar;

g) se debería restringir la conexión de los sistemas a la red.

Información adicional

En la ISO/IEC 27033. [15][16][17][18][19] se puede encontrar información adicional sobre la seguridad de la red.

13.1.2 Seguridad de los servicios de red

Control

Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Guía de implementación

La capacidad del proveedor de servicios de red para gestionar en forma segura los servicios acordados se debería determinar y hacerle seguimiento con regularidad, y se debería acordar el derecho a la auditoría.

Se deberían identificar los acuerdos de seguridad necesarios para los servicios particulares, tales como las características de seguridad, los niveles de servicio y los requisitos de gestión. La organización se debería asegurar de que los proveedores de servicio de redes implementen estas medidas.

Información adicional

Los servicios de red incluyen el suministro de conexiones, servicios de redes privadas y redes de valor agregado, y soluciones gestionadas de seguridad de redes tales como firewalls y sistemas de detección de intrusión. Estos servicios pueden comprender desde un ancho de banda no gestionado, a ofertas complejas de valor agregado.

Las características de seguridad de las redes de servicio pueden ser:

a) tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red;

b) los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;

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

13.1.3 Separación en las redes

Control

Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

Guía de implementación

Un método para gestionar la seguridad de las redes grandes es dividirlas en dominios de red separados. Los dominios se pueden escoger con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), junto con unidades organizacionales (por ejemplo, recursos humanos, finanzas, mercadeo) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples unidades organizacionales). La separación se puede hacer usando diferentes redes físicas o diferentes redes lógicas (por ejemplo, redes privadas virtuales).

El perímetro de cada dominio se debería definir bien. Se permite el acceso entre dominios de redes, pero se debería controlar en el perímetro usando un portal (por ejemplo, firewalls, enrutado de filtrado). Los criterios para la separación de redes en dominios, y el acceso permitido a través de los portales se debería basar en una valoración de los requisitos de seguridad de cada dominio. La valoración se debería hacer de acuerdo con la política de control de acceso (véase el numeral 9.1.1), los requisitos de acceso, el valor y la clasificación de la información procesada, y también tener en cuenta el costo relativo y el impacto que tiene para el desempeño la incorporación de tecnología de portal (*Gateway Portal*) adecuada.

Las redes inalámbricas requieren tratamiento especial debido a la pobre definición del perímetro de red. Para entornos sensibles, antes de conceder el acceso a los sistemas internos, se debería considerar tratar todos los accesos inalámbricos como conexiones externas y separar este acceso de las redes internas, hasta que el acceso haya pasado a través de un portal de acuerdo con la política de controles de redes (véase el numeral 13.1.1).

La autenticación, la criptografía y las tecnologías de control de acceso de redes a nivel de usuario, de las redes inalámbricas modernas basadas en estándares, pueden ser suficientes para dirigir la conexión directa a la red interna de la organización, cuando se implementa apropiadamente.

Información adicional

Con frecuencia las redes van más allá de los límites de la organización, ya que se forman sociedades de negocio que requieren la interconexión o intercambio de instalaciones para trabajo en red y procesamiento de información. Estas extensiones pueden incrementar el riesgo de acceso no autorizado a los sistemas de información de la organización que usan la red, algunos de los cuales requieren protección contra otros usuarios de la red, debido a su sensibilidad o criticidad.

13.2 TRANSFERENCIA DE INFORMACIÓN

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información

Control

Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

Guía de implementación

Los procedimientos y controles que se siguen cuando se usan instalaciones de comunicación para la transferencia de información deberían tener en cuenta los siguientes elementos:

a) los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción;

b) los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas (véase el numeral 12.2.1);

c) los procedimientos para proteger información electrónica sensible comunicada que está en forma de adjunto;

d) la política o directrices que presentan el uso aceptable de las instalaciones de comunicación (véase el numeral 8.1.3);

e) las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, por ejemplo, por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.;

f) el uso de técnicas criptográficas, por ejemplo, proteger la confidencialidad, la integridad y la autenticidad de la información (véase el numeral 10).

g) las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales;

h) los controles y restricciones asociadas con las instalaciones de comunicación, por ejemplo, el reenvío automático de correo electrónico a direcciones de correo externas;

i) brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial;

j) no dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta;

k) brindar asesoría al personal acerca de los problemas de usar máquinas o servicios de fax, a saber:

   1) acceso no autorizado para recuperar mensajes almacenados;

   2) programar las máquinas en forma deliberada o accidental para enviar mensajes a números específicos;

   3) enviar documentos y mensajes a un número equivocado, ya sea por marcación errada o por marcar un número almacenado equivocado.

Además, se le debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos, o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión.

Los servicios de transferencia de información deberían cumplir todos los requisitos legales pertinentes (véase el numeral 18.1).

Información adicional

Puede ocurrir transferencia de información mediante el uso de varios tipos diferentes de instalaciones de comunicación, incluido el correo electrónico, voz, fax y video.

La transferencia de software puede ocurrir a través de varios medios diferentes, incluida la descarga desde internet y la adquisición de productos en el comercio.

Se deberían considerar las implicaciones para el negocio, y las implicaciones legales y de seguridad asociadas con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, y los requisitos para los controles.

13.2.2 Acuerdos sobre transferencia de información

Control

Los acuerdos deberían tratar la transferencia segura de información del negocio entre la organización y las partes externas.

Guía de implementación

Los acuerdos de transferencia de información deberían incluir lo siguiente:

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

b) los procedimientos para asegurar trazabilidad y no repudio;

c) los estándares técnicos mínimos para empaquetado y transmisión;

d) certificados de depósito de títulos en garantía;

e) estándares de identificación de mensajería;

f) las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos;

g) el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente (véase el numeral 8.2);

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

i) cualquier control especial que se requiera para proteger elementos sensibles, tales como criptografía (véase el numeral 10);

j) mantener una cadena de custodia para la información mientras está en tránsito;

k) los niveles aceptables de control de acceso.

Se deberían establecer y mantener las políticas, procedimientos y estándares para proteger la información y los medios físicos en tránsito (véase el numeral 8.3.3), y se deberían referenciar en los acuerdos de transferencia.

El contenido de seguridad de la información de cualquier acuerdo debería reflejar el carácter sensible de la información del negocio involucrada.

Información adicional

Los acuerdos pueden ser electrónicos o manuales y pueden tomar la forma de contratos formales. Para información confidencial, los mecanismos específicos usados para la

transferencia de esta información deberían ser coherentes para todas las organizaciones y tipos de acuerdos.

13.2.3 Mensajería electrónica

Control

Se debería proteger adecuadamente la información incluida en la mensajería electrónica.

Guía de implementación

Las consideraciones de seguridad de la información para mensajería electrónica deberían incluir las siguientes:

a) la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización;

b) asegurar el direccionamiento y transporte correctos del mensaje;

c) la confiabilidad y disponibilidad del servicio;

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

e) la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información;

f) niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.

Información adicional

Hay muchos tipos de mensajería electrónica, tales como correo electrónico, intercambio electrónico de datos y redes sociales, que desempeñan un rol en las comunicaciones del negocio.

13.2.4 Acuerdos de confidencialidad o de no divulgación

Control

Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o de no divulgación deberían tener en cuenta el requisito de proteger la información confidencial usando términos ejecutables legalmente. Los acuerdos de confidencialidad o de no divulgación son aplicables a las partes externas o a empleados de la organización. Se deberían seleccionar o adicionar elementos teniendo en cuenta el tipo de la otra parte y su acceso o manejo permisible de la información confidencial. Con el fin de identificar los requisitos para los acuerdos de confidencialidad o de no divulgación, se deberían considerar los siguientes elementos:

a) una definición de la información que se va a proteger (información confidencial);

b) la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente;

c) las acciones requeridas cuando termina el acuerdo;

d) las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información;

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

f) el uso permitido de información confidencial y los derechos del firmante para usar la información;

g) el derecho a actividades de auditoría y de seguimiento que involucran información confidencial;

h) el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial;

i) los plazos para que la información sea devuelta o destruida al cesar el acuerdo;

j) las acciones que se espera tomar en caso de violación del acuerdo.

Con base en los requisitos de seguridad de la información de la organización, en un acuerdo de confidencialidad o de no divulgación pueden ser necesarios otros elementos.

Los acuerdos de confidencialidad y de no divulgación deberían cumplir todas las leyes y reglamentaciones aplicables para la jurisdicción pertinente (véase el numeral 18.1).

Los requisitos para los acuerdos de confidencialidad y de no divulgación se deberían revisar periódicamente, y cuando ocurran cambios que influyan en estos requisitos.

Información adicional

Los acuerdos de confidencialidad y de no divulgación protegen la información de la organización e informan a los firmantes acerca de su responsabilidad para proteger, usar y divulgar información de una manera autorizada y responsable.

La organización puede necesitar diferentes formas de acuerdos de confidencialidad o de no divulgación, en diferentes circunstancias.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Control

Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

Guía de implementación

Los requisitos de seguridad de la información se deberían identificar usando varios métodos, tales como la obtención de requisitos de cumplimiento a partir de políticas y reglamentación, modelado de amenazas, revisiones de incidentes, o uso de umbrales de vulnerabilidad. Los resultados de la identificación se deberían documentar y revisar por todas las partes interesadas.

Los requisitos y los controles de seguridad de la información deberían reflejar el valor que tiene para el negocio la información involucrada (véase el numeral 8.2) y el impacto negativo potencial para el negocio que podría resultar de la falta de seguridad adecuada.

La identificación y gestión de los requisitos de seguridad de la información y los procesos asociados se deberían integrar en las primeras etapas de los proyectos de sistemas de información. La consideración temprana de los requisitos de seguridad de la información, por ejemplo, en la etapa de diseño, puede conducir a soluciones más eficaces y eficientes en cuanto a costos.

Los requisitos de seguridad de la información también deberían considerar:

a) el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario.

b) los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos;

c) informar a los usuarios y operadores sobre sus deberes y responsabilidades;

d) las necesidades de protección requeridas de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad;

e) los requisitos derivados de los procesos del negocio, tales como registros de transacciones (*Transaction Loggins)* y seguimiento, y de no repudio;

f) los requisitos exigidos por otros controles de seguridad, por ejemplo, interfaces con el ingreso *(Logging*) o seguimiento, o los sistemas de detección de fuga de datos.

Para aplicaciones que suministran servicios en redes públicas o que implementan transacciones, se deberían considerar los controles dedicados 14.1.2 y 14.1.3.

Si los productos se adquieren, se debería seguir un proceso formal de adquisición y pruebas. Los contratos con los proveedores deberían tener en cuenta los requisitos de seguridad de la información. En donde la funcionalidad de la seguridad en un producto propuesto no satisface el requisito especificado, antes de comprar el producto se deberían reconsiderar el riesgo introducido y los controles asociados.

Se debería evaluar e implementar una guía disponible para configuración de la seguridad del producto, alineada con el software / servicio final *(Service Stack)* de ese sistema.

Los criterios para aceptar productos se deberían definir, por ejemplo, en términos de su funcionalidad, lo que dará seguridad de que los requisitos de seguridad identificados se cumplen. Los productos se deberían evaluar contra estos criterios, antes de su adquisición. Se debería revisar la funcionalidad adicional para asegurarse de que no introduce riesgos adicionales no aceptables.

Información adicional

La norma ISO/IEC 27005[11] y la norma NTC-ISO 31000[27] brindan orientación sobre el uso de procesos de gestión del riesgo para identificar los controles, para cumplir los requisitos de seguridad de la información.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Control

La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

Guía de implementación

Las consideraciones de seguridad de la información para servicios de aplicaciones que pasan sobre redes públicas deberían incluir las siguientes:

a) el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, por ejemplo, por medio de autenticación;

b) los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave;

c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio;

d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, por ejemplo, asociados con procesos de ofertas y contratos;

e) el nivel de confianza requerido en la integridad de los documentos clave;

f) los requisitos de protección de cualquier información confidencial;

g) la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos;

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

i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude;

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

k) evitar la pérdida o duplicación de información de la transacción;

l) la responsabilidad civil asociada con cualquier transacción fraudulenta;

m) los requisitos de seguros.

Muchas de las consideraciones anteriores se pueden abordar mediante la aplicación de controles criptográficos (véase numeral 10), teniendo en cuenta el cumplimiento de los requisitos legales (véase el numeral 18, véase especialmente 18.1.5 con relación a la legislación sobre criptografía).

Las disposiciones sobre servicio de aplicaciones (*Application Service Arrangements*) entre socios deberían estar apoyadas por un acuerdo documentado que comprometa a ambas partes bajo los términos de los servicios acordados, incluidos los detalles de la autorización (véase b) arriba).

Se deberían considerar los requisitos de resiliencia contra los ataques, que pueden incluir requisitos para proteger los servidores de las aplicaciones involucradas o asegurar la disponibilidad de las interconexiones de red requeridas para entregar el servicio.

Información adicional

Las aplicaciones accesibles por medio de redes públicas están sujetas a una variedad de amenazas relacionadas con la red, tales como actividades fraudulentas, disputas acerca de contratos, o divulgación de información al público. Por tanto, son indispensables las valoraciones de riesgo detalladas y la selección apropiada de controles. Los controles requeridos incluyen con frecuencia métodos criptográficos para la autenticación y seguridad en la transferencia de datos.

Los servicios de las aplicaciones (*Application Services*) pueden usar métodos de autenticación seguros, por ejemplo, el uso de una llave criptográfica pública y firmas digitales (véase el numeral 10) para reducir los riesgos. Además, cuando se necesiten estos servicios, se pueden usar terceras partes confiables.

14.1.3 Protección de transacciones de los servicios de las aplicaciones (*Application Services*)

Control

La información involucrada en las transacciones de los servicios de las aplicaciones (*Application Services*) se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Guía de implementación

Las consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones (*Application Service*) deberían incluir las siguientes:

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

b) todos los aspectos de la transacción, es decir, asegurar que:

1) la información de autenticación secreta de usuario (*User´s Secret Authentication Information*), de todas las partes, se valide y verifique;

2) la transacción permanezca confidencial;

3) se mantenga la privacidad asociada con todas las partes involucradas;

c) la trayectoria de las comunicaciones entre todas las partes involucradas esté cifrada;

d) los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados;

e) asegurarse de que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet;

f) en donde se use una autoridad confiable (por ejemplo, para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

Información adicional

El alcance de los controles adoptados necesita ser proporcional al nivel de riesgo asociado con cada forma de transacción de los servicios de las aplicaciones (*Application Service Transaction*).

Es posible que las transacciones tengan que cumplir requisitos legales y de reglamentaciones en la jurisdicción en la que se genera, se procesa, completa o almacena la transacción.

14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

14.2.1 Política de desarrollo seguro

Control

Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.

Guía de implementación

El desarrollo seguro es un requisito para crear un servicio, arquitectura, software o sistema seguros.

Dentro de una política de desarrollo seguro, se deberían considerar los siguientes aspectos:

a) la seguridad del ambiente de desarrollo;

b) la orientación sobre la seguridad en el ciclo de vida de desarrollo del software:

   1) la seguridad en la metodología de desarrollo de software;

   2) las directrices de codificación seguras para cada lenguaje de programación usado;

c) los requisitos de seguridad en la fase diseño;

d) los puntos de chequeo de seguridad dentro de los hitos del proyecto;

e) los depósitos seguros;

f) la seguridad en el control de la versión;

g) el conocimiento requerido sobre seguridad de la aplicación;

h) la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

Se deberían usar técnicas de programación seguras tanto para los nuevos desarrollos como para escenarios de reúso de códigos, en donde es posible que no se conozcan los estándares aplicados al desarrollo, o no sean coherentes con las mejores prácticas actuales. Se deberían considerar los estándares de codificación, y en donde sea pertinente, exigir su uso. Los desarrolladores deberían recibir formación para su uso y prueba, y su uso se debería verificar mediante la revisión de códigos.

Si el desarrollo es contratado externamente, la organización debería obtener seguridad de que la parte externa cumple estas reglas para un desarrollo seguro (véase el numeral 14.2.7).

Información adicional

El desarrollo también puede ocurrir dentro de las aplicaciones, tales como las aplicaciones de oficina, programación, navegadores y bases de datos.

14.2.2 Procedimientos de control de cambios en sistemas

Control

Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.

Guía de implementación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para asegurar la integridad del sistema, las aplicaciones y los productos, desde las primeras etapas de diseño a través de todos los esfuerzos de mantenimiento posteriores.

La introducción de nuevos sistemas y cambios importantes a los sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad y gestión de la implementación.

Este proceso debería incluir una valoración de riesgos, el análisis de los impactos de los cambios y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurar que los procedimientos de control y de seguridad existentes no se vean comprometidos, que a los programadores de soporte se les permita el acceso solamente a las partes del sistema necesarias para su trabajo, y que se obtiene el acuerdo y la aprobación formal para cualquier cambio.

Siempre que sea viable, se deberían integrar los procedimientos de control de cambios en aplicaciones y en operaciones (véase el numeral 12.1.2). Los procedimientos de control de cambios deberían incluir, entre otros:

a) llevar un registro de los niveles de autorización acordados;

b) asegurar que los cambios se presenten a los usuarios autorizados;

c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios;

d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección;

e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas;

f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience;

g) antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios;

h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se archiva, o se dispone de ella;

i) mantener un control de versiones para todas las actualizaciones de software;

j) mantener un rastro de auditoría (*Audit Trail*) de todas las solicitudes de cambio;

k) asegurar que la documentación de la operación (véase el numeral 12.1.1) y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados;

l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

Información adicional

El cambio de software puede tener impacto en el ambiente de producción y viceversa.

Las buenas prácticas incluyen probar el nuevo software en un ambiente separado tanto de los ambientes de producción como de desarrollo (véase el numeral 12.1.4). Esto permite tener control sobre el software nuevo y tener protección adicional de la información operacional que se usa para propósitos de pruebas. Esto debería incluir parches, paquetes de servicios y otras actualizaciones.

Cuando se consideran actualizaciones automáticas, el riesgo para la integridad y disponibilidad de sistema se debería sopesar contra el beneficio de un despliegue rápido de las actualizaciones. No se deberían usar actualizaciones automáticas en sistemas críticos, ya que algunas actualizaciones pueden hacer que fallen aplicaciones críticas.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Control

Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.

Guía de implementación

Este proceso debería comprender:

a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones;

b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación;

c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio (véase el numeral 17).

Información adicional

Las plataformas de operación incluyen sistemas operativos, bases de datos y plataformas de software intermedio (*Middleware Plataforms*). El control también se debería aplicar a los cambios en las aplicaciones.

14.2.4 Restricciones en los cambios a los paquetes de software

Control

Se deberían desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Guía de implementación

En cuanto sea posible y viable, se deberían usar paquetes de software suministrados por el vendedor-proveedor, que no hayan sufrido modificaciones. En donde un paquete de software necesite modificaciones, se deberían considerar los siguientes puntos:

a) el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos;

b) si se debería obtener el consentimiento del vendedor;

c) la posibilidad de obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar;

d) el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios;

e) la compatibilidad con otro software en uso.

Si los cambios son necesarios, el software original se debería conservar, y los cambios se deberían aplicar a la copia designada. Se debería implementar un proceso de gestión de actualizaciones de software para asegurar que se instalen las actualizaciones de aplicaciones y de parches aprobados más recientes para todo el software autorizado (véase el numeral 12.6.1). Todos los cambios se deberían probar y documentar completamente de manera que se puedan aplicar nuevamente, si es necesario, a futuras actualizaciones de software. Si se requiere, las modificaciones se deberían poner a prueba y validar por un organismo de evaluación independiente.

14.2.5 Principios de construcción de sistemas seguros

Control

Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Guía de implementación

Se deberían establecer, documentar y aplicar procedimientos de construcción de sistemas de información seguros basados en principios de construcción de seguridad, a actividades de construcción de sistemas de información internos. La seguridad se debería incluir en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de información, con la necesidad de accesibilidad. La nueva tecnología se debería analizar para determinar los riesgos para la seguridad, y el diseño se debería revisar contra patrones de ataque conocidos.

Estos principios y los procedimientos de construcción establecidos se deberían revisar con regularidad para asegurar que están contribuyendo efectivamente a mejorar los estándares de seguridad dentro del proceso de construcción. También se deberían revisar regularmente para asegurar que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los principios de construcción de seguridad de la información se deberían aplicar, en donde sea pertinente, a sistemas de información contratados externamente, por medio de contratos y otros acuerdos vinculantes entre la organización y el proveedor al que la organización contrata externamente. La organización debería confirmar que el rigor de los principios de construcción de seguridad de los proveedores es comparable con el suyo.

Información adicional

Los procedimientos de desarrollo de aplicaciones deberían aplicar técnicas de construcción seguras en el desarrollo de aplicaciones que tengan interfaces de entrada y de salida. Las técnicas de construcción segura brindan orientación sobre técnicas de autenticación de usuarios, control de sesiones seguras y validación de datos, desinfección y eliminación de códigos de depuración (*Debugging Codes*).

14.2.6 Ambiente de desarrollo seguro

Control

Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

Guía de implementación

Un ambiente de desarrollo seguro incluye personas, procesos y tecnología asociados con el desarrollo e integración de sistemas.

Las organizaciones deberían valorar los riesgos asociados con las labores de desarrollo de sistemas individuales y establecer ambientes de desarrollo seguros para las labores de desarrollo de sistemas específicos, considerando:

a) el carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir;

b) los requisitos externos e internos aplicables, por ejemplo, de reglamentaciones o políticas;

c) los controles de seguridad ya implementados por la organización, que brindan soporte al desarrollo del sistema;

d) la confiabilidad del personal que trabaja en el ambiente (véase el numeral 7.1.1);

e) el grado de contratación externa asociado con el desarrollo del sistema;

f) la necesidad de separación entre diferentes ambientes de desarrollo;

g) el control de acceso al ambiente de desarrollo;

h) el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí;

i) las copias de respaldo se almacenan en lugares seguros fuera del sitio;

j) el control sobre el movimiento de datos desde y hacia el ambiente.

Una vez que se determine el nivel de protección para un ambiente de desarrollo específico, las organizaciones deberían documentar los procesos correspondientes en procedimientos de desarrollo seguro, y suministrarlos a todos los individuos que los necesiten.

14.2.7 Desarrollo contratado externamente

Control

La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

Guía de implementación:

Cuando el desarrollo del sistema es contratado externamente, se deberían considerar los siguientes puntos en toda la cadena de suministro externa de la organización:

a) los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente (véase el numeral 18.1.2);

b) los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas (véase el numeral 14.2.1);

c) el suministro del modelo de amenaza aprobado, al desarrollador externo;

d) los ensayos de aceptación para determinar la calidad y exactitud de los entregables;

e) el suministro de evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad;

f) el suministro de evidencia de que se han hecho pruebas suficientes para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega;

g) el suministro de evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas;

h) certificados de depósito en garantía (*Escrow Arrangements*); por ejemplo, si el código fuente ya no está disponible;

i) derecho contractual con relación a procesos y controles de desarrollo de auditorías;

j) documentación eficaz del ambiente de construcción usado para crear entregables;

k) la organización sigue siendo responsable del cumplimiento con las leyes aplicables y con la verificación de la eficiencia del control.

Información adicional

En la norma ISO/IEC 27036[21][22][23] se puede encontrar información adicional sobre las relaciones con los proveedores.

14.2.8 Pruebas de seguridad de sistemas

Control

Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

Guía de implementación

Tanto los sistemas nuevos como los actualizados requieren pruebas y verificación completas durante los procesos de desarrollo, incluida la preparación de un programa detallado de actividades y entradas de las pruebas y salidas esperadas en una variedad de condiciones. Para desarrollos internos, estas pruebas las debería llevar a cabo inicialmente el equipo de desarrollo. Entonces se deberían llevar a cabo pruebas de aceptación independientes (tanto para desarrollos internos como para los contratados externamente) para asegurar que el sistema trabaja de la forma esperada y únicamente de esta manera (véanse 14.1.1 y 14.1.9). El alcance de la prueba debería ser proporcional a la importancia y naturaleza del sistema.

14.2.9 Prueba de aceptación de sistemas

Control

Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.

Guía de implementación

Las pruebas de aceptación del sistema deberían incluir las pruebas de requisitos de seguridad de la información (véanse 14.1.1 y 14.1.2) y la adherencia a prácticas de desarrollo seguro de sistemas (véase el numeral 14.2.1). Las pruebas también deberían llevarse a cabo sobre componentes recibidos y sistemas integrados. Las organizaciones pueden hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y deberían verificar que se han corregido los defectos relacionados con la seguridad.

Las pruebas se deberían llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente de la organización, y que las pruebas son confiables.

14.3 DATOS DE PRUEBA

Objetivo: Asegurar la protección de los datos usados para pruebas.

14.3.1 Protección de datos de prueba

Control

Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente.

Guía de implementación

Se debería evitar el uso de datos operacionales que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba. Si esta información de datos personales u otra información confidencial se usa para propósitos de las pruebas, todos los detalles y contenido sensibles se deberían proteger eliminándolos o modificándolos (véase la norma ISO/IEC 29101[26]).

Las siguientes directrices se deberían aplicar para la protección de los datos operacionales, cuando se usan con propósitos de pruebas:

a) los procedimientos de control de acceso, que se aplican a los ambientes de producción, se deberían aplicar también a los ambiente de pruebas

b) debería haber una autorización separada cada vez que se copia información operacional a un ambiente de pruebas;

c) la información operacional se debería borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas;

d) el copiado y uso de la información operacional se deberían registrar (*Logged)* para suministrar un rastro de auditoría (*Audit Trail*).

Información adicional

Las pruebas del sistema y de aceptación usualmente requieren volúmenes sustanciales de datos de ensayos que sean lo más cercanos posible a los datos operacionales.

15. RELACIONES CON LOS PROVEEDORES

15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con proveedores

Control

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.

Guía de implementación

La organización debería identificar y exigir controles de seguridad de la información para tener en cuenta en una política específicamente el acceso de los proveedores a la información de la organización. Estos controles deberían tener en cuenta los procesos y procedimientos que va a implementar la organización, al igual que los procesos y procedimientos que la organización debería exigir a sus proveedores que implementara, incluidos:

a) la identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, logísticos, servicios financieros, componentes de la infraestructura de TI, a quienes la organización permitirá acceso a su información;

b) un proceso y un ciclo de vida normalizado para la gestión de las relaciones con los proveedores;

c) la definición de los tipos de acceso a la información que se permitirá a diferentes tipos de proveedores, y el seguimiento y el control del acceso;

d) los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso, que sirvan como base para los acuerdos con proveedores individuales, con base en las necesidades y requisitos del negocio de la organización, y su perfil de riesgo;

e) los procesos y procedimientos para hacer seguimiento del cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por una tercera parte y la validación del producto;

f) los controles de exactitud y completitud, para asegurar la integridad de la información o del procesamiento de la información suministrada por una tercera parte;

g) los tipos de obligaciones aplicables a los proveedores para proteger la información de la organización;

h) el manejo de incidentes y contingencias asociadas con el acceso de proveedores, incluidas las responsabilidades tanto de la organización como de los proveedores;

i) la resiliencia, y si son necesarias, las disposiciones sobre recuperación y contingencias, para asegurar la disponibilidad de la información o el procesamiento de la información suministrada por cualquiera de las partes;

j) la formación sobre toma de conciencia, para el personal de la organización involucrado en adquisiciones, relativa a políticas, procesos y procedimientos aplicables;

k) la formación sobre toma de conciencia para el personal de la organización que interactúa con el personal de los proveedores, con respecto a las reglas apropiadas de interacción y comportamiento, con base en el tipo de proveedor, y en el nivel de acceso del proveedor a los sistemas e información de la organización;

l) las condiciones bajo las cuales los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;

m) la gestión de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que sea necesario mover, y asegurar que la seguridad de la información se mantiene durante todo el período de transición.

Información adicional

La información puede estar en riesgo cuando los proveedores tienen una gestión de seguridad de la información inadecuada. Se deberían identificar los controles y aplicarlos para administrar el acceso de los proveedores a las instalaciones de procesamiento de información. Por ejemplo, si hay una necesidad especial de confidencialidad de la información, se pueden usar los acuerdos de no divulgación. Otro ejemplo son los riesgos de protección de datos, cuando el acuerdo con los proveedores incluye la transferencia o acceso de información a través de fronteras. La organización necesita tener conciencia de que la responsabilidad legal o contractual con respecto a la protección sigue siendo de la organización.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

Control

Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Guía de implementación

Se deberían establecer y documentar acuerdos con los proveedores para asegurar que no haya malos entendidos entre la organización y el proveedor con respecto a las obligaciones de ambas partes con relación al cumplimiento de los requisitos de seguridad de la información pertinentes.

Los siguientes términos se deberían considerar para inclusión en los acuerdos, con el fin de satisfacer los requisitos de seguridad de la información identificados:

a) una descripción de la información que se va a suministrar o a la que se va a tener acceso, y los métodos para suministrar la información o para acceder a ella;

b) la clasificación de la información de acuerdo con el esquema de clasificación de la organización (véase el numeral 8.2); si es necesario, también el mapeo entre el propio esquema de clasificación de la organización, y el esquema de clasificación del proveedor;

c) los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se asegurará que se cumplan;

d) la obligación de cada parte contractual de implementar y acordar un grupo de controles que incluyan controles de acceso, revisión del desempeño, seguimiento, reporte y auditoría;

e) las reglas de uso aceptable de la información, incluido el uso inaceptable, si es necesario;

f) una lista explícita de personal del proveedor autorizado para tener acceso a la información de la organización o recibirla de ella, o los procedimientos o condiciones para la autorización, y el retiro de la autorización para el acceso o recibo de información de la organización por parte del personal del proveedor;

g) las políticas de seguridad de la información pertinentes al contrato específico;

h) los requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la remediación de incidentes);

i) los requisitos de formación y toma de conciencia para procedimientos específicos, y los requisitos de seguridad de la información, por ejemplo, para respuesta a incidentes, procedimientos de autorización;

j) las reglamentaciones pertinentes para contratación externa, incluidos los controles que es necesario implementar;

k) los socios pertinentes en los acuerdos, incluida una persona de contacto, para asuntos de seguridad de la información;

l) requisitos de selección, si los hay, para el personal del proveedor, incluidas las responsabilidades para la realización de la selección, y los procedimientos de notificación, si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud;

m) el derecho de auditar los procesos y controles de los proveedores, relacionados con el acuerdo;

n) los procesos de solución de defectos y resolución de conflictos;

o) la obligación de los proveedores de entregar periódicamente un informe independiente sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes presentados en el informe;

p) las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.

Información adicional

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre diferentes tipos de proveedores. Por tanto, se debería prestar atención para incluir todos los requisitos y riesgos de seguridad de la información pertinentes. Los acuerdos con los proveedores también pueden incluir a otras partes (por ejemplo, partes contratadas externamente).

En el acuerdo es necesario considerar los procedimientos para continuar el procesamiento en caso de que el proveedor llegue a ser incapaz de suministrar sus productos o servicios, para evitar cualquier retraso en disponer el reemplazo de productos o servicios.

15.1 3 Cadena de suministro de tecnología de información y comunicación

Control

Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Guía de implementación

Los siguientes temas se deberían considerar para inclusión en los acuerdos con los proveedores, concernientes a la seguridad de la cadena de suministro:

a) definir los requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología de la información y de comunicaciones, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores;

b) para los servicios de tecnología de información y de comunicaciones, exigir que los proveedores divulguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro, si los proveedores contratan externamente partes del servicio de tecnología de la información y comunicaciones que suministran a la organización;

c) para los productos de tecnología de información y comunicaciones, exigir que los proveedores divulguen prácticas de seguridad adecuadas a lo largo de la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores;

d) implementar un proceso de seguimiento y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos de seguridad establecidos;

e) implementar un proceso para identificar los componentes de los productos o servicios que son críticos para mantener la funcionalidad, y por tanto, requieren una mayor atención y escrutinio cuando se construyen por fuera de la organización, especialmente si el proveedor en el nivel superior contrata externamente aspectos de componentes de productos o servicios a otros proveedores;

f) obtener la seguridad de que los componentes críticos y su origen se pueden rastrear a todo lo largo de la cadena de suministro;

g) obtener seguridad de que los productos de tecnología de información y de comunicación están funcionando en la forma esperada, sin ningún aspecto indeseado o inesperado:

h) definir reglas para compartir información concerniente a la cadena de suministro y cualquier problema y compromisos entre la organización y los proveedores;

i) implementar procesos específicos para la gestión del ciclo de vida y la disponibilidad de componentes de tecnología de información y de comunicación, y de los riesgos de seguridad asociados. Esto incluye la gestión de riesgos de componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o ya no suministran estos componentes debido a que se han hecho avances en la tecnología.

Información adicional

Las prácticas específicas de gestión de riesgos en la cadena de suministro de tecnología de información y de comunicación se desarrollan sobre prácticas generales de construcción de sistemas y de gestión de proyectos, de calidad y seguridad de la información, pero no los reemplazan.

Es conveniente que las organizaciones trabajen con proveedores que comprendan la cadena de suministro de tecnología de información y comunicación y cualquier asunto que tenga un impacto importante sobre los productos y servicios que se suministran. Las organizaciones pueden influir en las prácticas de seguridad de la información de la cadena de suministro de tecnología de información y comunicación, estableciendo en forma clara en los acuerdos con sus proveedores, los temas que deberían tener en cuenta otros proveedores en la cadena de suministro de tecnología de información y comunicación.

La cadena de suministro de tecnología de información y comunicación como se aborda aquí, incluye los servicios de cómputo en la nube.

15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Control

Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

Guía de implementación

El seguimiento y la revisión de los servicios de los proveedores deberían asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionen apropiadamente.

Esto debería involucrar un proceso de relacionamiento para la gestión del servicio entre la organización y el proveedor para:

a) hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos;

b) revisar los reportes de servicio elaborados por el proveedor, y concertar reuniones de avance regulares, según se exija en los acuerdos;

c) llevar a cabo auditorías de los proveedores, junto con la revisión de reportes de auditores independientes, si están disponibles, y seguimiento a las cuestiones identificadas;

d) suministrar información acerca de incidentes de seguridad de la información y revisar esta información según se exija en los acuerdos y en cualquier directriz y procedimiento de soporte;

e) revisar los rastros de auditoría (*Audit Trails*) del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con el servicio entregado;

f) resolver y gestionar cualquier problema identificado;

g) revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus propios proveedores;

h) asegurar que el proveedor mantenga una capacidad de servicio suficiente, junto con planes ejecutables destinados a asegurar que se mantienen los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre (véase el numeral 17).

La responsabilidad de la gestión de las relaciones con los proveedores se debería asignar a un individuo o equipo de gestión de servicio designado. Además, la organización debería asegurar que los proveedores asignen responsabilidades para la revisión de la conformidad y velen por el cumplimiento de los requisitos de los acuerdos. Debería haber disponibles suficientes recursos y habilidades técnicas para hacer seguimiento del cumplimiento de los requisitos del acuerdo, en particular, los requisitos de seguridad de la información. Se deberían tomar las acciones apropiadas cuando se observen deficiencias en la entrega del servicio.

La organización debería mantener suficiente control y visibilidad general sobre todos los aspectos de seguridad para la información sensible o crítica o para las instalaciones de procesamiento de información a las que se tiene acceso, procesadas o gestionadas por un proveedor. La organización debería mantener visibilidad en áreas de seguridad tales como gestión de cambios, identificación de vulnerabilidades y reporte y respuesta de incidentes de seguridad de la información, a través de un proceso de reporte definido.

15.2.2 Gestión de cambios en los servicios de los proveedores

Control

Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

Guía de implementación

Se deberían considerar los siguientes aspectos:

a) los cambios en los acuerdos con los proveedores;

b) los cambios hechos por la organización para implementar:

1) las mejoras a los servicios ofrecidos en la actualidad;

2) el desarrollo de nuevas aplicaciones y sistemas;

3) las modificaciones o actualizaciones a las políticas y procedimientos de la organización;

4) los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad;

c) los cambios en los servicios de los proveedores para implementar:

1) cambios y mejoras en las redes;

2) el uso de nuevas tecnologías;

3) la adopción de nuevos productos o versiones/ediciones más recientes;

4) nuevas herramientas y ambientes de desarrollo;

5) cambios en las ubicaciones físicas de las instalaciones de servicio;

6) cambio de proveedores;

7) contratación externa de otros proveedores.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Guía de implementación

Se deberían considerar las siguientes directrices para responsabilidades y procedimientos de gestión con relación a la gestión de incidentes de seguridad de la información:

a) se deberían establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:

1) los procedimientos para la planificación y preparación de respuesta a incidentes;

2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información;

3) procedimientos para registrar (*Logging*) las actividades de gestión de incidentes;

4) procedimientos para el manejo de evidencia forense;

5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información;

6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior (escalamiento), recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas;

b) los procedimientos establecidos deberían asegurar que:

1) personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización;

2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad;

3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información;

c) los procedimientos de reporte deberían incluir:

1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información;

2) el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, por ejemplo, tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas;

3) referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad;

4) los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.

Los objetivos de la gestión de incidentes de seguridad de la información se deberían acordar con la dirección, y se debería asegurar que los responsables de la gestión de incidentes de seguridad de la información comprenden las prioridades de la organización para el manejo de incidentes de seguridad de la información.

Información adicional

Los incidentes de seguridad de la información podrían transcender las fronteras organizacionales y nacionales. Para responder a estos incidentes hay una necesidad creciente de coordinar las respuestas y compartir información acerca de estos incidentes con las organizaciones externas, según el caso.

Para orientación detallada sobre la gestión de incidentes de seguridad de la información, véase la GTC-ISO/IEC 27035[20].

16.1.2 Reporte de eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.

Guía de implementación

Todos los empleados y contratistas deberían tomar conciencia de su responsabilidad de reportar eventos de seguridad de la información tan pronto como sea posible. También deberían ser conscientes del procedimiento para reportar eventos de seguridad de la información y el punto de contacto al que se deberían reportar los eventos.

Las situaciones que se deberían considerar para el reporte de eventos de seguridad de la información incluyen:

a) un control de seguridad ineficaz;

b) violación de la integridad, confidencialidad o expectativas de disponibilidad de la información;

c) errores humanos;

d) no conformidades con políticas o directrices;

e) violaciones de acuerdos de seguridad física;

f) cambios no controlados en el sistema;

g) mal funcionamiento en el software o hardware;

h) violaciones de acceso.

Información adicional

El mal funcionamiento u otro comportamiento anómalo del sistema puede ser un indicador de un ataque a la seguridad o una violación real a la seguridad, y por lo tanto se debería reportar siempre como un evento de seguridad de la información.

16.1.3 Reporte de debilidades de seguridad de la información

Control

Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Guía de implementación

Todos los empleados y contratistas deberían reportar estos asuntos al punto de contacto lo más pronto posible, para evitar incidentes de seguridad de la información. El mecanismo de reporte debería ser lo más sencillo, accesible y disponible posible.

Información adicional

Se debería advertir a empleados y contratistas que no intenten poner a prueba las debilidades de seguridad sospechadas. Esto podría ser interpretado como un mal uso potencial del sistema y podría causar daño al sistema o servicio de información y derivar en responsabilidad legal para el individuo que haga estas pruebas.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Control

Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.

Guía de implementación

El punto de contacto debería evaluar cada evento de seguridad de la información usando la escala acordada de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento se debería clasificar como un incidente de seguridad de la información. La clasificación y priorización de incidentes puede ayudar a identificar el impacto y la extensión de un incidente.

En los casos en que la organización cuente con un equipo de respuesta a incidentes de seguridad de la información (ERISI), la evaluación y la decisión se pueden enviar al ERISI para confirmación o revaloración.

Los resultados de la evaluación y la decisión se deberían registrar en detalle para referencia y verificación futuras.

16.1.5 Respuesta a incidentes de seguridad de la información

Control

Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Guía de implementación

Un punto de contacto designado y otras personas pertinentes de la organización o partes externas deberían responder a los incidentes de seguridad de la información (véase el numeral 16.1.1)

La respuesta debería incluir lo siguiente:

a) recolectar evidencia lo más pronto posible después de que ocurra el incidente;

b) Llevar a cabo análisis forense de seguridad de la información, según se requiera (véase el numeral 16.1.7);

c) Llevar el asunto a una instancia superior (escalar), según se requiera;

d) Asegurarse de que todas las actividades de respuesta involucradas se registren (*Logged*) adecuadamente para análisis posterior;

e) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo;

f) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente;

g) una vez que el incidente se haya tratado exitosamente, cerrarlo formalmente y hacer un registro de esto.

Se debería llevar a cabo un análisis posterior al incidente, según sea necesario, para identificar su origen.

Información adicional

La primera meta de la respuesta a incidentes es reanudar el “nivel de seguridad normal” e iniciar la recuperación necesaria.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Control

El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

Guía de implementación

Se debería contar con mecanismos que permitan cuantificar y hacer el seguimiento de todos los tipos, volúmenes y costos de incidentes de seguridad de la información. La información obtenida de la evaluación de incidentes de seguridad de la información se debería usar para identificar los incidentes recurrentes o con impacto alto.

Información adicional

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de controles adicionales o mejorados para limitar la frecuencia, daño y costo de futuros sucesos, o

ser tenida en cuenta en el proceso de revisión de la política de seguridad (véase el numeral 5.1.2).

Prestando la debida atención a los aspectos de confidencialidad, las anécdotas de los incidentes de seguridad de la información reales se pueden usar en la formación de toma de conciencia (véase el numeral 7.2.2) como ejemplos de lo que podría ocurrir, cómo responder a estos incidentes y cómo evitarlos en el futuro.

16.1.7 Recolección de evidencia

Control

La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Guía de implementación

Se deberían desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias.

En general, estos procedimientos para evidencia deberían suministrar procesos de identificación, recolección, adquisición y preservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendidos o apagados. Los procedimientos deberían tener en cuenta:

a) la cadena de custodia;

b) la seguridad de la evidencia;

c) la seguridad del personal;

d) los roles y responsabilidades del personal involucrado;

e) la competencia del personal;

f) la documentación;

g) las sesiones informativas.

Cuando esté disponible, se debería buscar una certificación u otro medio pertinente de calificación del personal y herramientas, para fortalecer el valor de la evidencia preservada.

La evidencia forense puede trascender los límites organizacionales o jurisdiccionales. En estos casos, se debería asegurar que la organización esté autorizada para recolectar la información requerida como evidencia forense. Los requisitos de las diferentes jurisdicciones también se deberían considerar para maximizar las oportunidades de admisión a través de las jurisdicciones pertinentes.

Información adicional

La identificación es el proceso que involucra la búsqueda, reconocimiento y documentación de evidencia potencial. Recolección es el proceso de reunir elementos físicos que pueden contener evidencia potencial.

Adquisición es el proceso de crear una copia de los datos dentro de un grupo definido. Preservación es el proceso de mantener y salvaguardar la integridad y la condición original de la evidencia potencial.

Cuando se detecta por primera vez un evento de seguridad de la información, tal vez no sea obvio si el evento dará como resultado una acción judicial. Por tanto, existe el peligro de que la evidencia necesaria se destruya intencional o accidentalmente antes de darse cuenta de la gravedad del incidente. Es recomendable involucrar a un abogado o a la policía al comienzo de cualquier acción legal contemplada, y aceptar asesoría acerca de la evidencia requerida.

La norma ISO/IEC 27037[24] proporciona directrices para la identificación, recolección, adquisición y preservación de evidencia digital.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información

Control

La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Guía de implementación

Una organización debería determinar si la continuación de la seguridad de la información se ha incluido dentro del proceso de gestión de continuidad de negocio o dentro del proceso de gestión para recuperación de desastres. Los requisitos de seguridad de la información se deberían determinar cuándo se planifican la continuidad de negocio y la recuperación en caso de desastres.

En ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas.

Información adicional

Con el fin de reducir el tiempo y el esfuerzo que implica un análisis “adicional” del impacto en el negocio de la seguridad de la información, se recomienda capturar los aspectos de seguridad de la información dentro de la gestión normal de la continuidad de negocio, o el análisis de impacto en el negocio de la recuperación de desastres. Esto implica que los requisitos de continuidad de seguridad de la información se formulan explícitamente en los procesos de continuidad de negocio o de gestión de recuperación de desastres.

La información sobre la gestión de la continuidad de negocio se puede encontrar en las normas ISO/IEC 27031[14] ISO 22313[9] e ISO 22301[8].

17.1.2 Implementación de la continuidad de la seguridad de la información

Control

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Guía de implementación

Una organización debería asegurar que:

a) se cuente con una estructura de gestión adecuada para prepararse, mitigar y responder a un evento perturbador usando personal con la autoridad, experiencia y competencia necesarias.

b) se nombre personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.

c) se desarrollen y aprueben planes, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento perturbador y mantendrá su seguridad de la información en un nivel predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección (véase el numeral 17.1.1).

De acuerdo con los requisitos de continuidad de la seguridad de la información, la organización debería establecer, documentar, implementar y mantener:

a) los controles de la seguridad de la información dentro de procesos de continuidad de negocio o recuperación de desastres, y sistemas y herramientas de apoyo;

b) los cambios en los procesos, procedimientos e implementación, para mantener los controles de seguridad de la información existentes, durante una situación adversa;

c) los controles de compensación para los controles de seguridad de la información que no se pueden mantener durante una situación adversa.

Información adicional

Dentro del contexto de continuidad de negocio o recuperación de desastres, se pueden haber definido procesos y procedimientos específicos. Se debería proteger la información que es manejada dentro de estos procesos y procedimientos, o dentro de sistemas de información dedicados que los apoyan. Por tanto, una organización debería involucrar especialistas en seguridad de la información cuando se establecen, implementan y mantienen procesos y procedimientos de continuidad de negocio o de recuperación de desastres.

Los controles de seguridad de la información que se han implementado deberían continuar operando durante una situación adversa. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Control

La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Guía de implementación

Los cambios organizacionales, técnicos, procedimentales y de los procesos, ya sea en un contexto operacional o de continuidad, pueden conducir a cambios en los requisitos de continuidad de la seguridad de la información. En estos casos, la continuidad de los procesos, procedimientos y controles para seguridad de la información se debería revisar contra los requisitos que han sufrido cambios.

Las organizaciones deberían verificar la continuidad de la gestión de la seguridad de su información:

a) ejercitando y poniendo a prueba la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información;

b) ejercitando y poniendo a prueba el conocimiento y rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que su desempeño es coherente con los objetivos de continuidad de la seguridad de la información;

c) revisando la validez y la eficacia de las medidas de continuidad de la seguridad de la información cuando cambian los sistemas de información, los procesos, procedimientos y controles de seguridad de la información, o los procesos y soluciones de gestión de continuidad de negocio/recuperación de desastres.

Información adicional

La verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información, y se debería llevar a cabo aparte de las pruebas que se llevan a cabo cuando hay cambios. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de continuidad de negocio y recuperación de desastres de la organización.

17.2 REDUNDANCIAS

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Control

Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Guía de implementación

Las organizaciones deberían identificar los requisitos del negocio para la disponibilidad de los sistemas de información. Cuando no se puede garantizar disponibilidad usando la arquitectura de los sistemas existentes, se deberían considerar componentes o arquitecturas redundantes.

Cuando sea aplicable, los sistemas de información redundante se deberían poner a prueba para asegurar que después de una falla, la conmutación (*Failover*) de un componente a otro funcione de la forma prevista.

Información adicional

La implementación de las redundancias puede introducir riesgos a la integridad o confidencialidad de la información y de los sistemas de información, y es necesario considerarla cuando se diseñan sistemas de información.

18. CUMPLIMIENTO

18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.

Guía de implementación

Además, se deberían documentar los controles y las responsabilidades individuales específicas para cumplir estos requisitos.

Los gerentes deberían identificar toda la legislación aplicable a su organización para cumplir los requisitos para su tipo de negocio. Si la organización hace negocios en otros países, los gerentes deberían considerar el cumplimiento en todos los países pertinentes.

18.1.2 Derechos de propiedad intelectual

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

Guía de implementación

Las siguientes directrices se deberían considerar para la protección de cualquier material que se pueda considerar propiedad intelectual:

a) publicar una política de cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos;

b) adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violan los derechos de autor;

c) mantener conciencia de las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias contra el personal que las incumpla;

d) mantener los registros de activos apropiados, e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual;

e) mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.

f) implementar controles para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia;

g) llevar a cabo revisiones acerca de que solo hay instalados software autorizado y productos con licencia;

h) suministrar una política para mantener las condiciones de licencia apropiadas;

i) suministrar una política para disposición o transferencia de software a otros;

j) cumplir con los términos y condiciones para el software y la información obtenida de las redes públicas;

k) no duplicar, convertir a otro formato o extraer de registros comerciales (video, audio) más allá de lo que permita la ley de derechos de autor;

l) no copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.

Información adicional

Los derechos de propiedad intelectual incluyen derechos de autor de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuente.

Los productos de software patentados usualmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitar el uso de productos a máquinas especificadas, o limitar la copia únicamente a la creación de copias de respaldo. La importancia de los derechos de propiedad intelectual y la toma de conciencia sobre estos se debería comunicar al personal, para el software desarrollado por la organización.

Los requisitos legislativos, de reglamentación y contractuales pueden poner restricciones al copiado de material patentado. En particular, pueden exigir que solamente se use material desarrollado por la organización o que tenga licencia del desarrollador o haya sido suministrado por éste. La violación de los derechos de autor puede conducir a acciones legales que pueden involucrar multas y procesos penales.

18.1.3 Protección de registros

Control

Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

Guía de implementación

Cuando se decide proteger los requisitos específicos de la organización, se debería considerar su clasificación correspondiente, basada en el esquema de clasificación de la organización. Los registros se deberían clasificar por tipos de registros, por ejemplo, registros contables, registros de bases de datos, registros de transacciones (*Logs*), registros de auditoría (*Audit Logs*) y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos. Cualquier llave criptográfica y programas relacionados asociados con archivos cifrados o firmas digitales (véase el numeral 10), también se deberían almacenar para permitir el descifrado de los registros durante el tiempo en que están retenidos.

Se debería considerar la posibilidad de deterioro de los medios usados para el almacenamiento de registros. Se deberían implementar procedimientos de almacenamiento y manejo, de acuerdo con las recomendaciones de los fabricantes.

Cuando se escogen medios de almacenamiento electrónico, se deberían establecer procedimientos para acceder a los datos (legilibilidad de medios y de formatos) durante todo el período de retención, para proteger contra pérdida debidos a cambios futuros en la tecnología.

Se deberían escoger sistemas de almacenamiento de datos de manera que los datos requeridos se puedan recuperar en un tiempo y formato aceptables, dependiendo de los requisitos que se deben cumplir.

El sistema de almacenamiento y manejo debería asegurar la identificación de los registros y de su período de retención, como se define en la legislación o reglamentaciones nacionales o regionales. Este sistema debería permitir la destrucción apropiada de registros después de ese período, si la organización ya no los necesita.

Para cumplir estos objetivos de salvaguarda de registros, se deberían realizar los siguientes pasos dentro de la organización:

a) se deberían emitir directrices acerca de la retención, almacenamiento, manejo y disposición de registros e información;

b) se debería elaborar un programa de retención que identifique los registros y el período de tiempo durante el cual se deberían retener;

c) se debería llevar un inventario de fuentes de información clave.

Información adicional

Puede ser necesario retener en forma segura algunos registros, para cumplir con requisitos estatutarios, de reglamentación o contractuales, al igual que para brindar apoyo a actividades de negocio esenciales. Algunos ejemplos incluyen registros que se pueden solicitar como evidencia de que una organización opera dentro de las disposiciones estatutarias o de

reglamentación, para asegurar la defensa contra acciones civiles o criminales potenciales, o para confirmar el estado financiero de una organización a los accionistas, partes interesadas y auditores. Las leyes o reglamentaciones nacionales pueden ajustar el período de tiempo y el contenido de los datos para retención de información.

En la norma NTC-ISO/IEC 15489-1[5] se puede encontrar información adicional sobre gestión de registros de la organización.

18.1.4 Privacidad y protección de información de datos personales.

Control

Se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

Guía de implementación

Se debería desarrollar e implementar una política relativa a datos de la organización, para la privacidad y la protección de datos personales. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información de datos personales.

El cumplimiento de esta política y de toda la legislación y reglamentación pertinente concerniente a la protección de la privacidad de las personas y a la protección de los datos personales requiere una estructura y control de gestión apropiados. Con frecuencia, la mejor manera de lograrlo es nombrando una persona responsable, como por ejemplo el funcionario encargado de la privacidad, quien debería brindar orientación a los gerentes, usuarios y proveedores de servicios acerca de sus responsabilidades individuales y de los procedimientos específicos que se deberían seguir. La responsabilidad por el manejo de información sobre datos personales y por asegurar la toma de conciencia sobre los principios de privacidad se debería abordar de acuerdo con la legislación y las reglamentaciones pertinentes. Se deberían implementar medidas técnicas y organizacionales para proteger la información de datos personales.

Información adicional

La ISO/IEC 29100[25] presenta un marco de referencia de alto nivel para la protección de información de datos personales dentro de los sistemas de tecnología de la información y de la comunicación. Varios países han introducido legislación que establece controles sobre la recolección, procesamiento y transmisión de información de datos personales (generalmente información sobre individuos vivos que pueden ser identificados a partir de esa información). Dependiendo de la legislación nacional respectiva, estos controles pueden imponer deberes a quienes recolectan, procesan y divulgan información de datos personales, y pueden también restringir la capacidad de transferir información de datos personales a otros países.

18.1.5 Reglamentación de controles criptográficos

Control

Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

Guía de implementación

Se deberían considerar los siguientes aspectos para el cumplimiento con los acuerdos, leyes y reglamentaciones:

a) las restricciones sobre importación o exportación de hardware y software, para la realización de funciones criptográficas;

b) las restricciones sobre importación o exportación de hardware y software que está diseñado para la adición de funciones criptográficas;

c) las restricciones sobre el uso de criptografía;

d) los métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a información cifrada mediante software o hardware para brindar confidencialidad al contenido.

Se debería buscar asesoría legal para asegurar el cumplimiento con la legislación y las reglamentaciones pertinentes. Antes de que la información cifrada o los controles criptográficos atraviesen fronteras jurisdiccionales, también se debería buscar asesoría legal.

18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

18.2.1 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

Guía de implementación

La dirección debería dar inicio a una revisión independiente. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la organización para gestionar la seguridad de la información. Esta revisión debería incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

Esta revisión la deberían llevar a cabo individuos independientes del área que se revisa, por ejemplo, la función de auditoría interna, un gerente independiente o una parte externa de la organización que se especializa en estas revisiones. Los individuos que llevan a cabo estas revisiones deberían contar con las habilidades y experiencia apropiadas.

Los resultados de la revisión independiente se deberían registrar y reportar a la dirección que dio inicio a la revisión. Se deberían mantener estos registros.

Si la revisión independiente identifica que el enfoque y la implementación de la organización para la gestión de la seguridad de la información son inadecuados, por ejemplo, no se cumplen los objetivos y requisitos documentados, o no cumplen con la orientación sobre seguridad de la

información establecida en las políticas de seguridad de la información (véase el numeral 5.1.1), la dirección debería considerar acciones correctivas.

Información adicional

La norma ISO/IEC 27007[12], "*Guidelines for Information Security Management Systems Auditing*" e ISO/IEC TR 27008[13], "*Guidelines for Auditors on Information Security Controls*" también suministran orientación para llevar a cabo la revisión independiente.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Control

Los gerentes deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

Guía de implementación

Los gerentes deberían identificar cómo revisar que se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y otras reglamentaciones aplicables. Para una revisión eficiente, se debería considerar herramientas automáticas para medición y reporte.

Si se encuentra alguna no conformidad como resultado de la revisión, los gerentes deberían:

a) identificar las causas de la no conformidad, y

b) evaluar la necesidad de acciones para lograr cumplimiento:

c) implementar las acciones correctivas apropiadas;

d) revisar la acción correctiva tomada, para verificar su eficacia e identificar cualquier deficiencia o debilidad.

Los resultados de las revisiones y de las acciones correctivas realizadas por la dirección, deberían ser registradas y estos registros se deberían mantener. Los gerentes deberían reportar los resultados a las personas que llevan a cabo revisiones independientes (véase el numeral 18.2.1) cuando se realiza una revisión independiente en su área de responsabilidad.

Información adicional

En el numeral 12.4 se trata sobre el seguimiento operacional del uso del sistema.

18.2.3 Revisión del cumplimiento técnico

Control

Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Guía de implementación

El cumplimiento técnico se debería revisar, preferiblemente con la ayuda de herramientas automáticas que generan informes técnicos para la interpretación posterior por un especialista

técnico. Como alternativa, un ingeniero de sistemas experimentado puede llevar a cabo revisiones manuales (si es necesario, con el apoyo de herramientas de software apropiadas).

Si se usan pruebas de penetración (*Penetration Test*) o valoraciones de vulnerabilidad, es necesario tener precaución, ya que estas actividades pueden comprometer la seguridad del sistema. Estas pruebas se deberían planificar, documentar, y deberían ser repetibles.

Cualquier revisión de cumplimiento técnico solo lo deberían llevar a cabo personas competentes autorizadas, o bajo la supervisión de dichas personas.

Información adicional

Las revisiones del cumplimiento técnico involucran examinar los sistemas operacionales para asegurar que los controles de hardware y de software se han implementado correctamente. Este tipo de revisión de cumplimiento requiere pericia técnica especializada.

Las revisiones de cumplimiento también deberían comprender, por ejemplo, las pruebas de penetración (*Penetration Test*) y las valoraciones de vulnerabilidad, que se podrían llevar a cabo por expertos independientes contratados específicamente para este propósito. Esto puede ser útil para detectar vulnerabilidades en el sistema y para examinar la eficacia de los controles para evitar el acceso no autorizado debido a estas vulnerabilidades.

Las pruebas de penetración (*Penetration Test*) y las valoraciones de vulnerabilidad dan un panorama inmediato de un sistema en un estado específico, en un momento específico. Este panorama está limitado a las porciones del sistema sometidas a pruebas realmente durante el(los) intento(s) de penetración. Las pruebas de penetración (*Penetration Test*) y las valoraciones de vulnerabilidad no son un sustituto de la valoración de riesgos.

La ISO/IEC TR 27008[13] suministra orientación específica sobre revisiones de cumplimiento técnico.

BIBLIOGRAFÍA

[1] ISO/IEC Directives, Part 2.

[2] ISO/IEC 11770-1, *Information Technology Security Techniques. Key Management. Part 1: Framework.*

[3] ISO/IEC 11770-2, *Information Technology. Security Techniques. Key Management. Part 2: Mechanisms Using Symmetric Techniques.*

[4] ISO/IEC 11770-3, *Information Technology. Security Techniques. Key management. Part 3: Mechanisms Using Asymmetric Techniques.*

[5] NTC-ISO 15489-1, Información y documentación. Gestión de documentos. Parte 1. Generalidades

[6] NTC-ISO/IEC 20000-1, Tecnología de la información. Gestión del servicio. Parte 1: requisitos del sistema de gestión del servicio.

[7] ISO/IEC 20000-2[1], *Information Technology. Service Management. Part 2: Guidance on the Application of Service Management Systems.*

[8] ISO 22301, *Societal Security. Business Continuity Management Systems. Requirements.*

[9] ISO 22313, *Societal Security. Business Continuity Management Systems. Guidance.*

[10] NTC-ISO/IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

[11] ISO/IEC 27005, *Information Technology. Security Techniques. Information Security Risk Management.*

[12] ISO/IEC 27007, *Information Technology. Security Techniques. Guidelines for Information Security Management Systems Auditing.*

[13] ISO/IEC TR 27008, *Information Technology. Security Techniques. Guidelines for Auditors on Information Security Controls.*

[14] ISO/IEC 27031, *Information Technology. Security Techniques. Guidelines for Information and Communication Technology Readiness for Business Continuity.*

[15] ISO/IEC 27033-1, *Information Technology. Security Techniques. Network Security. Part 1: Overview and Concepts.*

[16] ISO/IEC 27033-2, *Information Technology. Security Techniques. Network Security. Part 2: Guidelines for the Design and Implementation of Network Security.*

[17] ISO/IEC 27033-3, *Information Technology. Security Techniques. Network Security. Part 3: Reference Networking Scenarios. Threats, Design Techniques and Control Issues.*

[1] La ISO/IEC 20000-2:2005, fue cancelada y reemplazada por la ISO/IEC 20000-2:2012, Information Technology. Service Management. Part 2: Guidance on the application of Service Management Systems.

[18] ISO/IEC 27033-4, *Information Technology. Security Techniques. Network Security. Part 4: Securing Communications Between Networks Using Security Gateways.*

[19] ISO/IEC 27033-5, *Information Technology. Security Techniques. Network security. Part 5: Securing Communications Across Networks Using Virtual Private Network (VPNs).*

[20] GTC-ISO/IEC 27035, Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.

[21] ISO/IEC 27036-1, *Information Technology. Security Techniques. Information Security for Supplier Relationships. Part 1: Overview and Concepts.*

[22] ISO/IEC 27036-2, *Information Technology. Security techniques. Information Security for Supplier Relationships. Part 2: Common Requirements.*

[23] ISO/IEC 27036-3, *Information Technology. Security Techniques. Information Security for Supplier Relationships. Part 3: Guidelines for ICT Supply Chain Security.*

[24] ISO/IEC 27037, *Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.*

[25] ISO/IEC 29100, *Information Technology. Security Techniques. Privacy Framework.*

[26] ISO/IEC 29101, *Information Technology. Security Techniques. Privacy Architecture Framework.*

[27] NTC-ISO 31000, Gestión del riesgo. Principios y directrices.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information Technology. Security Techniques. Code of Practice for Information Security Controls.* Geneva: ISO, 2013, 90 p. (ISO/IEC 27002:2013 (E) + Technical Corrigendum 1: 2014).

GUÍA TÉCNICA COLOMBIANA GTC-ISO/IEC 27035

2012-12-12

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E: INFORMATION TECHNOLOGY. SECURITY TECHNIQUES. INFORMATION SECURITY INCIDENT MANAGEMENT.

CORRESPONDENCIA:	esta guía es una adopción idéntica (IDT) de la norma ISO/IEC 27035: 2011.
DESCRIPTORES:	tecnología de la información; técnicas de seguridad; información; seguridad de la información; incidente; gestión de incidentes.

I.C.S.: 35.040

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

 Editada 2012-12-21

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La guía GTC-ISO/IEC 27035 fue ratificada por el Consejo Directivo de 2012-12-12.

Esta guía está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta guía a través de su participación en el Comité Técnico 181 Gestión de T.I..

ARCHIVO GENERAL DE LA NACIÓN
AVIANCA
BANCO AGRARIO DE COLOMBIA S.A.
BANCO DE LA REPUBLICA
CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES -CCIT-
CAMARA DE COMERCIO DE MEDELLÍN
CENET S.A.
CROSS BORDER TECHNOLOGY S.A.S.
FIDUCIARIA POPULAR
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR -ICBF-
IQ INFORMATION QUALITY
LIGHT SKY LTDA.
MAREIGUA
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
NEWNET S.A.
OUTSOURCING S.A.
PROJECT ADVANCED MANAGEMENT
SELTIKA
SERVIENTREGA S.A.
SOANSES LTDA.
SUN GEMINI S.A.
TELMEX S.A.
TOP FACTORY S.A.
UNIVERSIDAD AUTÓNOMA OCCIDENTE

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

A TODA HORA S.A ATH
ACH COLOMBIA S.A.
ACTUALIZACIONES DE SISTEMAS LTDA.
AEROVÍAS DEL CONTINENTE AMERICANO S.A. -AVIANCA S.A.-
AGENDA DE CONECTIVIDAD
ALFA COMPRESIÓN
ALIANZA SINERTIC
BANCO CAJA SOCIAL
BANCO COMERCIAL AV VILLAS
BANCO DAVIVIENDA S.A.
BANCO DE BOGOTÁ
BRANCH OF MICROSOFT COLOMBIA INC
CAJA COLOMBIANA DE SUBSIDIO FAMILIAR COLSUBSIDIO
CENTRO DE INVESTIGACIÓN Y DESARROLLO EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

CENTRO POLICLÍNICO DEL OLAYA
C.P.O. S.A.
CHOUCAIR TESTING S.A.
CIBERCALL S.A.
COLOMBIA TELECOMUNICACIONES S.A. E.S.P.
COMERCIO ELECTRÓNICO EN INTERNET CENET S.A.
COMPUREDES S.A.
CONTRALORÍA DE CUNDINAMARCA
COOPERATIVA DE PROFESIONALES DE LA SALUD -PROSALCO I.P.S.-
CREDIBANCO
DAKYA LTDA.
ECOPETROL S.A.
ENLACE OPERATIVO S.A.
ETB S.A. E.S.P.
FLUIDSIGNAL GROUP S.A.
FONDO DE EMPLEADOS DEL DEPARTAMENTO DE ANTIOQUIA
FUNDACIÓN PARQUE TECNOLÓGICO DEL SOFTWARE DE CALI -PARQUESOFT-
FUNDACIÓN UNIVERSITARIA INPAHU
GESTIÓN & ESTRATEGIA S.A.S.
GETRONICS COLOMBIA LTDA.
GIT LTDA.
HERRAMIENTAS PARA EL MEJORAMIENTO DEL TRABAJO LTDA.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
INFOCOMUNICACIONES S.A.S.
INFOTRACK S.A.
INSTITUTO DE ORTOPEDIA INFANTIL ROOSEVELT
IPX LTDA.
IQ CONSULTORES
IT SERVICE LTDA.
JAIME TORRES C. Y CÍA. S.A.
JIMMY EXENOVER ESPINOSA LÓPEZ
KEXTAS LTDA.
LOGIN LEE LTDA.
MAKRO SUPERMAYORISTA S.A.
MAREIGUA LTDA.
MEGABANCO
MICROCOM COMUNICACIÓN Y SEGURIDAD LTDA.
NEGOTEC NEGOCIOS Y TECNOLOGÍA LTDA.
NEXIA
NEXOS SOFTWARE S.A.S.
PARQUES Y FUNERARIAS S.A.
JARDINES DEL RECUERDO
PIRAMIDE ADMINISTRACIÓN DE INFORMACIÓN LTDA.
POLITÉCNICO MAYOR AGENCIA CRISTIANA DE SERVICIO Y EDUCACIÓN LTDA.
PONTIFICIA UNIVERSIDAD JAVERIANA
QUALITY SYSTEMS LTDA.
SENA
SISTEMAS Y FORMACIÓN S.A.S.
SOCIEDAD COLOMBIANA DE ARCHIVISTAS
SYNAPSIS COLOMBIA LTDA.
TEAM FOODS COLOMBIA S.A.
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE COLOMBIA LTDA.
TELMEX COLOMBIA S.A.
TIQAL S.A.S.
TOMÁS MORENO CRUZ Y CÍA. LTDA.
TRANSFIRIENDO S.A.
TRANSPORTADORA DE VALORES ATLAS LTDA.
TUS COMPETENCIAS LTDA.
UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
UNIVERSIDAD JAVERIANA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNIVERSIDAD NACIONAL DE COLOMBIA
UNIVERSIDAD SANTIAGO DE CALI

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

PRÓLOGO

ISO (la Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado de normalización mundial. Los organismos nacionales que son miembros de ISO o de IEC participan en el desarrollo de normas internacionales a través de los comités establecidos por la respectiva organización para tratar los campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en unión con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el comité ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las directivas de ISO/IEC.

La principal labor del comité técnico conjunto es preparar normas internacionales. Las versiones preliminares de las normas internacionales adoptadas por el comité técnico conjunto se dan a conocer a todos los organismos nacionales para su votación. La publicación como una Norma Internacional requiere la aprobación de mínimo el 75 % de los organismos miembro que votan.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no asumen responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La norma ISO/IEC 27035 fue elaborada por el comité técnico conjunto ISO/IEC JTC 1, *Tecnología de la información*, subcomité SC 27, *Técnicas de seguridad de IT.*

Esta primera edición reemplaza a la GTC 169 (ISO/IEC TR 18044:2004), la cual se ha sometido a revisión técnica.

CONTENIDO

Página

INTRODUCCIÓN 1

1. OBJETO Y CAMPO DE APLICACIÓN 2

2. REFERENCIAS NORMATIVAS 2

3. TÉRMINOS Y DEFINICIONES 2

4. VISIÓN GENERAL 3

4.1 CONCEPTOS BÁSICOS 3

4.2 OBJETIVOS 4

4.3 BENEFICIOS DE UN ENFOQUE ESTRUCTURADO 5

4.4 ADAPTABILIDAD 7

4.5 FASES 8

4.6 EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 9

5. FASE DE PLANIFICACIÓN Y PREPARACIÓN 10

5.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE 10

5.2 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 13

5.3 INTEGRACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN OTRAS POLÍTICAS 16

5.4 ESQUEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 17

5.5 ESTABLECIMIENTO DEL ISIRT 24

Página

5.6 SOPORTE TÉCNICO Y OTRO (INCLUIDO EL SOPORTE OPERATIVO) 25

5.7 TOMA DE CONCIENCIA Y FORMACIÓN 27

5.8 PRUEBA DEL ESQUEMA DE ATENCIÓN DE INCIDENTES 29

6. FASE DE DETECCIÓN Y REPORTE 29

6.1 VISIÓN GENERAL SOBRE LAS ACTIVIDADES CLAVE 29

6.2 DETECCIÓN DE EVENTOS.....32

6.3 REPORTE DE EVENTOS 33

7. FASE DE EVALUACIÓN Y DECISIÓN 35

7.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE 35

7.2 EVALUACIÓN Y DECISIÓN INICIAL POR EL PoC (PUNTO DE CONTACTO) 36

7.3 EVALUACIÓN Y CONFIRMACIÓN DEL INCIDENTE POR EL ISIRT 39

8. FASE DE RESPUESTAS 41

8.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE 41

8.2 RESPUESTAS.....43

9. FASE DE LECCIONES APRENDIDAS 52

9.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE 52

9.2 ANÁLISIS FORENSE DE SEGURIDAD DE LA INFORMACIÓN ADICIONALES 53

9.3 IDENTIFICACIÓN DE LAS LECCIONES APRENDIDAS.....53

9.4 IDENTIFICACIÓN Y MEJORAS EN LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN 55

Página

9.5 IDENTIFICACIÓN Y MEJORAS A LOS RESULTADOS DE LA REVISIÓN POR LA DIRECCIÓN Y DE LA EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....55

9.6 IDENTIFICACIÓN Y MEJORAS EN EL ESQUEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 55

9.7 OTRAS MEJORAS 56

BIBLIOGRAFÍA.....94

DOCUMENTO DE REFERENCIA.....96

ANEXO A (Informativo)
TABLA DE REFERENCIAS CRUZADAS ENTRE LA NTC-ISO/IEC 27001 Y LA GTC-ISO/IEC 27035.....57

ANEXO B (Informativo)
EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y SUS CAUSAS.....60

ANEXO C (Informativo)
EJEMPLO DE ENFOQUES PARA LA CATEGORIZACIÓN Y CLASIFICACIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 64

ANEXO D (Informativo)
REPORTES Y FORMULARIOS DE EVENTOS, INCIDENTES Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN.....78

ANEXO E (Informativo)
ASPECTOS LEGALES Y REGLAMENTARIOS 91

FIGURAS

Figura 1. Relación entre los objetos en una cadena de incidentes de seguridad de la información.....4

Figura 2. Fases de la gestión de incidentes de seguridad de la información 9

Figura 3. Diagrama de flujo de eventos e incidentes de seguridad de la información.....30

TECNOLOGÍA DE LA INFORMACIÓN.
TÉCNICAS DE SEGURIDAD.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

En general, las políticas o controles de seguridad de la información por sí solas no garantizan la protección total de la información, de los sistemas de información, o de los servicios o redes. Después de que los controles se han implementado, es posible que queden vulnerabilidades residuales que pueden hacer ineficaz la seguridad de la información y, en consecuencia, hacer posibles incidentes de seguridad de la información. Potencialmente, esto puede tener impactos adversos directos e indirectos sobre las operaciones de los negocios de una organización, que pueden conducir inevitablemente a que ocurran nuevos casos de amenazas no identificadas previamente. Una preparación insuficiente de una organización para abordar este tipo de incidentes hará que cualquier respuesta sea menos eficaz, y que se incremente el grado de impacto adverso potencial en el negocio. Por tanto, es esencial que cualquier organización con interés auténtico en la seguridad de la información, tenga un enfoque estructurado y planificado para:

- detectar, reportar y evaluar incidentes de seguridad de la información;

- responder a incidentes de seguridad de la información, incluida la activación de controles adecuados para la prevención y la reducción de impactos, y la recuperación de ellos (por ejemplo, en el soporte para las área de gestión de crisis);

- reportar las vulnerabilidades de seguridad de la información que aún no han sido aprovechadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, evaluarlas y tratarlas adecuadamente;

- aprender de los incidentes y vulnerabilidades de seguridad de la información, implementar controles preventivos y hacer mejoras al enfoque global para la gestión de incidentes de seguridad de la información.

La presente guía brinda orientación sobre la gestión de incidentes de seguridad de la información, del numeral 4 al 9. Estos numerales constan de varios subnumerales que incluyen una descripción detallada de cada fase.

La expresión "gestión de incidentes de seguridad de la información” se usa en la presente guía para abarcar no sólo la gestión de incidentes de seguridad de la información, sino también las vulnerabilidades de la seguridad de la información.

1. OBJETO Y CAMPO DE APLICACIÓN

La presente guía brinda un enfoque estructurado y planificado para:

a) detectar, reportar y evaluar incidentes de seguridad de la información;

b) responder a incidentes de seguridad de la información y hacer su gestión;

c) detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información, y

d) mejorar continuamente la seguridad de la información y la gestión de incidentes como resultado de la gestión de los incidentes y vulnerabilidades de seguridad de la información.

La presente guía brinda orientación sobre la gestión de incidentes de seguridad de la información para empresas grandes y medianas. Las organizaciones más pequeñas pueden usar un conjunto básico de documentos, procesos y rutinas descritos en la presente guía, de acuerdo con su tamaño y tipo de negocio, en relación con la situación de riesgo de seguridad de la información. También brinda orientación para organizaciones externas que prestan servicios de gestión de incidentes de seguridad de la información.

2. REFERENCIAS NORMATIVAS

El siguiente documento referenciado es indispensable para la aplicación de este documento. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la última edición del documento referenciado (incluida cualquier enmienda).

ISO/IEC 27000, *Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.*

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de esta guía se aplican los términos y definiciones presentados en la ISO/IEC 27000 y los siguientes:

3.1 Investigación forense de seguridad de la información (*Information Security Forensics*). Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

3.2 Equipo de respuesta a incidentes de seguridad de la información, ISIRT (*por sus siglas en inglés Information Security Incident Response Team*). Equipo conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de éstos.

NOTA como se describe en esta guía el ISIRT, es una función organizacional que abarca el proceso para atender incidentes de seguridad de la información y se enfoca principalmente en incidentes relacionados con TI. Otras funciones comunes (con abreviaturas similares) dentro del manejo de incidentes pueden tener un alcance y propósito ligeramente diferentes. Las siguientes siglas de uso común tienen un significado similar al del ISIRT, aunque no exactamente igual.

CERT (por sus siglas en inglés *Computer Emergency Response Team*), Equipo de respuesta ante emergencias de tecnología de información; se enfoca principalmente en incidentes de tecnología de información y comunicaciones. Puede haber otras definiciones nacionales específicas para el CERT.

CSIRT (por sus siglas en inglés *Computer Security Incident Response Team*), Equipo de respuesta a incidentes de seguridad de tecnología de la información; es una organización de servicio responsable de recibir, examinar y responder a reportes y actividades de incidentes de seguridad de tecnología de la información. Estos servicios se llevan a cabo usualmente para un grupo definido, que puede ser una entidad matriz tal como una corporación, organización gubernamental u organización educativa, una región o país, una red de investigación, o un cliente que paga por estos servicios.

3.3 Evento de seguridad de la información. Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

[ISO/IEC 27000:2009]

3.4 Incidente de seguridad de la información. Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

[ISO/IEC 27000:2009]

4. VISIÓN GENERAL

4.1 CONCEPTOS BÁSICOS

Un evento de seguridad de la información es la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación a la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. Un incidente de seguridad de la información es un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de poner en riesgo las operaciones del negocio y de amenazar la seguridad de la información.

La ocurrencia de un evento de seguridad de la información no significa necesariamente que un intento haya tenido éxito, o que haya implicaciones para la confidencialidad, la integridad y/o la disponibilidad, es decir, no todos los eventos de seguridad de la información se clasifican como incidentes de seguridad de la información.

NOTA Intento no implica intencionalidad. Éste también podría ser accidental.

Una amenaza actúa de formas inesperadas para aprovecharse de las vulnerabilidades de los sistemas, servicios o redes de información, esto es la ocurrencia de eventos de seguridad de la información y tiene el potencial de causar incidentes no deseados, a los activos de información expuestos por las vulnerabilidades. La Figura 1 muestra esta relación de objetos, en una cadena de incidentes de seguridad de la información. Los objetos sombreados son preexistentes, afectados por los objetos no sombreados en la cadena, que da como resultado un incidente de seguridad de la información.

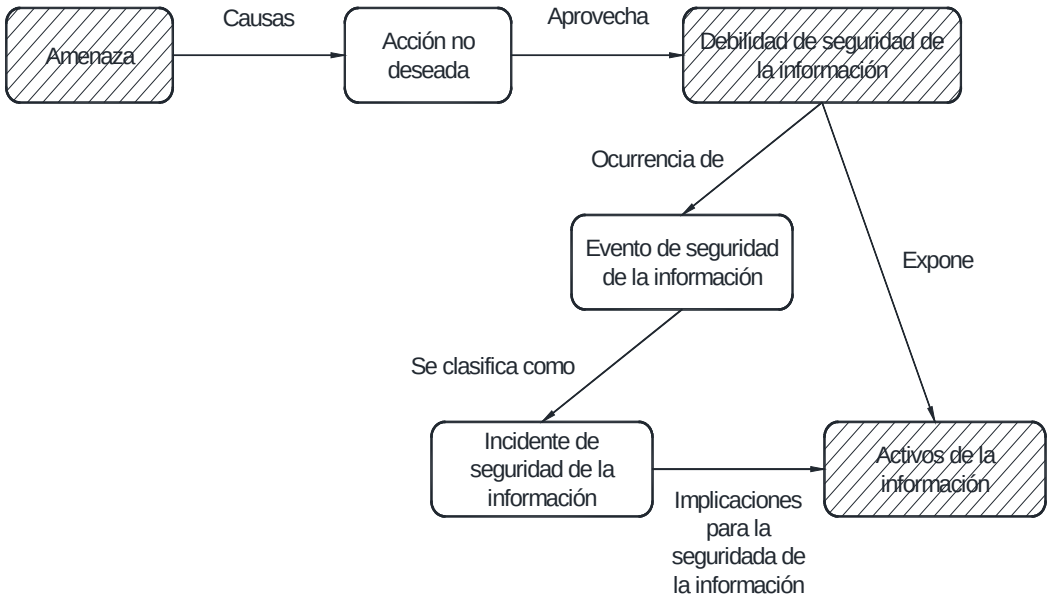

Figura 1. Relación entre los objetos en una cadena de incidentes de seguridad de la información

4.2 OBJETIVOS

Como una parte clave de la estrategia global de seguridad de la información de la organización, ésta debería implementar controles y procedimientos para posibilitar un enfoque estructurado y bien planificado para la gestión de incidentes de seguridad de la información. Desde la perspectiva del negocio, el objetivo principal es evitar o contener el impacto de los incidentes de seguridad de la información para reducir los costos directos e indirectos causados por los incidentes.

Los pasos fundamentales para minimizar el impacto negativo directo de los incidentes de seguridad de la información son los siguientes:

- detectar y contener;
- eliminar;
- analizar y reportar, y
- hacer seguimiento.

Los objetivos de un enfoque estructurado y bien planificado, son más refinados y deberían asegurar lo siguiente:

a) que los eventos de seguridad de la información se detecten y traten en forma eficiente, en particular identificando si es necesario categorizarlos y clasificarlos o no como incidentes de seguridad de la información;

b) que los incidentes de seguridad de la información identificados se evalúen y se les dé respuesta de la manera más eficiente y adecuada;

c) que los efectos adversos de los incidentes de seguridad de la información sobre la organización y las operaciones de sus negocios se minimicen, mediante los controles adecuados como parte de la respuesta a incidentes, en lo posible junto con los elementos pertinentes de un plan o planes de gestión de crisis;

d) que las vulnerabilidades de seguridad de la información reportadas, sean evaluadas y tratadas adecuadamente;

e) que las lecciones de los incidentes de seguridad de la información, vulnerabilidades y gestión asociada se aprendan rápidamente, para incrementar las oportunidades de evitar que ocurran futuros incidentes de seguridad de la información, mejorar la implementación y uso de controles de seguridad de la información y mejorar el esquema general de gestión de incidentes de seguridad de la información.

Para que esto se logre, las organizaciones deberían asegurarse de que los incidentes de seguridad de la información estén documentados, de manera consistente, mediante estándares adecuados para categorización y clasificación de incidentes, y se intercambie información con las partes pertinentes, de manera que se creen métricas a partir de datos agregados durante un periodo de tiempo. De esta manera, se brinda información valiosa para ayudar al proceso de toma de decisiones estratégicas cuando se invierte en controles de seguridad de la información.

Se reitera que otro objetivo asociado con la presente guía es brindar orientación a las organizaciones que buscan cumplir los requisitos de la norma NTC-ISO/IEC 27001 (y por tanto, con la orientación de la NTC-ISO/IEC 27002). Esto incluye los requisitos relacionados con gestión de incidentes de seguridad de la información. En el Anexo A (informativo) se presenta una tabla que muestra una comparación entre los numerales de la norma NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002, y los numerales de esta guía.

4.3 BENEFICIOS DE UN ENFOQUE ESTRUCTURADO

Una organización que usa un enfoque estructurado para la gestión de incidentes de seguridad de la información obtendrá beneficios significativos que se pueden agrupar de la siguiente manera:

a) Mejora de la seguridad global de la información

Un proceso estructurado para la detección, reporte, evaluación y toma de decisiones acerca de eventos e incidentes de seguridad de la información permitirá su rápida identificación y respuesta. De esta manera mejorará la seguridad global, al ayudar a identificar e implementar rápidamente una solución consistente y suministrar mecanismos de prevención de futuros incidentes de seguridad de información similares. Además, se obtendrán beneficios gracias a las métricas y a compartir y agregar la información. La credibilidad de la organización mejorará mediante la demostración de la implementación de mejores prácticas, con respecto a la gestión de incidentes de seguridad de la información.

b) Reducción de impactos adversos para el negocio

Un enfoque estructurado para la gestión de incidentes de seguridad de la información puede ayudar a reducir el nivel de los impactos adversos para el negocio, asociados con incidentes de seguridad de la información. Estos impactos pueden incluir una pérdida financiera inmediata y pérdida a largo plazo, a causa del daño en la reputación

y en la credibilidad (para orientación sobre el análisis de impacto en el negocio, véase la NTC-ISO/IEC 27005:2008).

c) Fortalecimiento del enfoque en prevención de incidentes de seguridad de la información

El uso de un enfoque estructurado para la gestión de incidentes de seguridad ayuda a crear un mejor enfoque para la prevención de incidentes dentro de la organización, incluidos los métodos de identificación de nuevas amenazas y vulnerabilidades. El análisis de datos relacionados con incidentes permitiría la identificación de patrones y tendencias, facilitando así un enfoque más exacto sobre prevención de incidentes y así, la identificación de las acciones adecuadas para evitar que ocurran incidentes.

d) Fortalecimiento de la priorización

Un enfoque estructurado para la gestión de incidentes de seguridad de la información brindará una base sólida para la priorización, cuando se llevan a cabo investigaciones de incidentes de seguridad de la información, incluido el uso de escalas de categorización y clasificación eficaces. Si no hay procedimientos claros, existe el riesgo de que las actividades de investigación se lleven a cabo de manera reactiva, respondiendo a incidentes a medida que éstos ocurren y pasando por alto las actividades que son necesarias llevar a cabo. De esta manera, se impediría que las actividades de investigación se dirijan a áreas en las que pueda haber mayor prioridad y en donde realmente se necesitan y en la prioridad apropiada.

e) Fortalecimiento de la evidencia

Contar con procedimientos claros para investigación de incidentes puede ayudar a asegurar que la recolección y el manejo de datos sean evidentemente acertados y admisibles legalmente. Estas son consideraciones importantes, en caso de que pudiera emprenderse una acción disciplinaria o legal. Sin embargo, debe reconocerse que existe la posibilidad de que las acciones necesarias para recuperarse de un incidente de seguridad de la información puedan poner en peligro la integridad de la evidencia recolectada.

f) Contribución a las justificaciones de presupuesto y de recursos

Un enfoque bien definido y estructurado para la gestión de incidentes de seguridad de la información ayudará a justificar y simplificar la asignación de presupuestos y recursos dentro de las áreas involucradas. Además, será mayor el beneficio para el propio esquema de gestión de incidentes de seguridad de la información mediante:

- el uso de personal menos calificado en la identificación y filtrado de alarmas de anormalidad o anomalía,

- una mejor orientación a las actividades del personal calificado y

- la participación del personal calificado sólo en aquellos procesos en los que se necesiten sus habilidades y solamente en la etapa del proceso en que sea necesaria su contribución.

Otro enfoque útil para controlar y optimizar el presupuesto y los recursos es agregar seguimiento al tiempo de gestión de incidentes para facilitar las evaluaciones cuantitativas del manejo de incidentes de seguridad de la información. Por ejemplo, debería ser posible suministrar información sobre el tiempo que toma resolver incidentes

de seguridad de la información de diferentes prioridades y en diferentes plataformas. Si existen represamientos en el proceso de gestión de incidentes de seguridad de la información, también deberían ser identificables.

g) Mejora de actualizaciones a los resultados de la evaluación y la gestión de riesgos de seguridad de la información.

El uso de un enfoque estructurado para la gestión de incidentes de seguridad de la información facilitará:

- una mejor recolección de datos para ayudar a identificar y determinar las características de los diversos tipos de amenazas y vulnerabilidades asociadas, y

- el suministro de datos sobre frecuencias de ocurrencia de los tipos de amenaza identificados.

Los datos recolectados sobre los impactos adversos en las operaciones del negocio, por incidentes de seguridad de la información, serán útiles en el análisis de impacto en el negocio. Los datos recolectados para identificar la frecuencia de ocurrencia de los diversos tipos de amenaza ayudarán considerablemente a la calidad de la evaluación de las amenazas. En forma similar, los datos recolectados sobre vulnerabilidades ayudarán considerablemente a la calidad de las futuras evaluaciones de vulnerabilidades (para orientación acerca de la evaluación y gestión de riesgos de seguridad de la información, véase la norma NTC-ISO/IEC 27005:2008).

h) Mejora en la conciencia en seguridad de la información y el material del programa de entrenamiento.

Un enfoque estructurado para la gestión de incidentes de seguridad de la información proporcionará información orientada a programas de toma de conciencia en seguridad de la información. Esta información suministrará ejemplos reales que demuestran que los incidentes de seguridad de la información le ocurren a organizaciones reales. También será posible demostrar los beneficios asociados con la rápida disponibilidad de información sobre soluciones. Además, esta toma de conciencia ayuda a reducir los errores o pánico o confusión de un individuo en caso de un incidente de seguridad de la información.

i) Suministro de entradas para las revisiones de la política de seguridad de la información y documentación relacionada.

Los datos suministrados por un esquema de gestión de incidentes de seguridad de la información pueden brindar entradas valiosas para las revisiones de la eficacia y de la posterior mejora de las políticas de seguridad de la información (y otros documentos de seguridad de la información relacionados). Esto se aplica a políticas y otros documentos aplicables tanto a la organización como a los sistemas, servicios y redes individuales.

4.4 ADAPTABILIDAD

La orientación que suministra la presente guía es de gran alcance, y si se adopta completamente puede requerir recursos significativos para su operación y gestión. Por tanto, es importante que una organización que aplica esta guía mantenga un sentido de la perspectiva y se asegure de que los recursos aplicados a la gestión de incidentes de seguridad de la

información y a la complejidad de los mecanismos implementados se mantienen en proporción a lo siguiente:

a) tamaño, estructura y naturaleza del negocio de una organización;

b) el alcance de cualquier sistema de gestión de seguridad de la información dentro del cual se manejan los incidentes;

c) el potencial de pérdida debido a incidentes no previstos, y

d) las metas del negocio.

Por tanto, una organización que utiliza esta guía debería adoptar su orientación en debida proporción a la escala y características de su negocio.

4.5 FASES

Para lograr los objetivos planteados en el numeral 4.2, la gestión de incidentes de seguridad de la información consta de las cinco fases siguientes:

- planificación y preparación,
- detección y reporte,
- evaluación y decisión,
- respuestas, y
- lecciones aprendidas.

La primera fase involucra tener en su lugar todo lo que se requiere para que la gestión de incidentes de seguridad de la información se lleve a cabo de manera exitosa. Las otras cuatro fases involucran el uso operativo de la gestión de incidentes de seguridad de la información.

En la Figura 2 se presenta una visión general de estas fases.

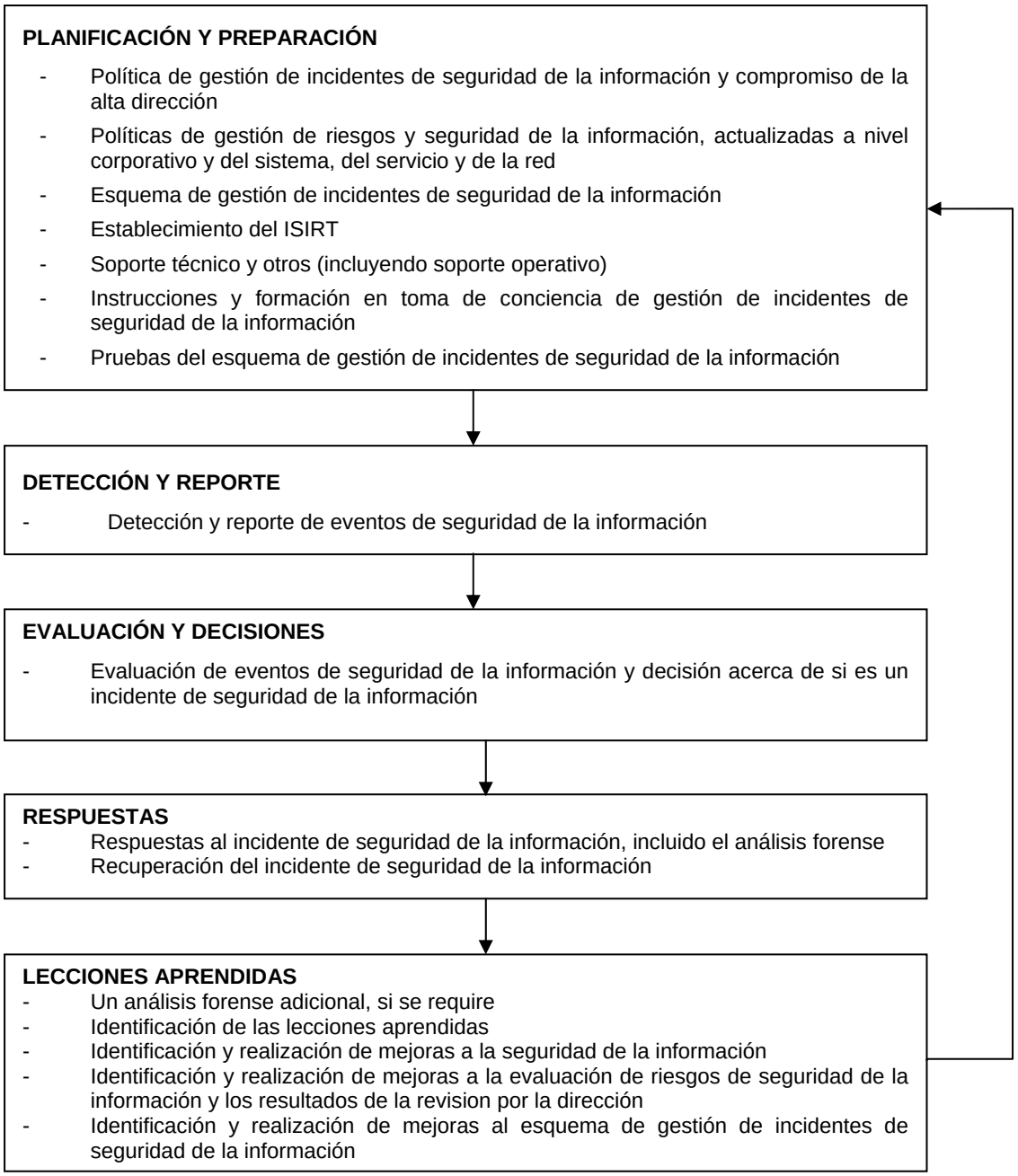

Figura 2. Fases de la gestión de incidentes de seguridad de la información

4.6 EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad pueden ser deliberados o accidentales (por ejemplo, causados por error o por acción de la naturaleza), y pueden ser causados por medios técnicos o físicos. Sus consecuencias pueden incluir la divulgación, la modificación, la destrucción o no disponibilidad de información de manera no autorizada, o daño o robo de activos de la organización. Si se determina que los eventos de seguridad de la información no reportados son incidentes, resulta difícil investigar los incidentes y tomar el control para impedir su recurrencia.

El Anexo B (informativo) presenta descripciones de ejemplos de incidentes de seguridad de la información y sus causas, con fines de información únicamente. Es importante tener en cuenta que estos ejemplos no son exhaustivos de ninguna manera.

5. FASE DE PLANIFICACIÓN Y PREPARACIÓN

5.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE

Una gestión eficaz de incidentes de seguridad de la información requiere planificación y preparación adecuadas. Para que un esquema eficaz y eficiente de la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información sea puesto en uso, la organización debería llevar a cabo varias actividades preparatorias, después de la planificación necesaria. La organización debería asegurar que las actividades de la fase de planificación y preparación incluyan:

a) Actividad para formular y generar una política de gestión de eventos/incidentes/vulnerabilidades de seguridad de la información y lograr el compromiso de la alta dirección con esa política. Ésta debería ir precedida de una revisión de la seguridad de las vulnerabilidades de la organización, confirmación de la necesidad de un esquema de gestión de incidentes de seguridad de la información, e identificación de los beneficios para la organización entera y para sus departamentos (véase el numeral 5.2). Asegurar el compromiso continuo de la dirección es vital para la aceptación de un enfoque estructurado para la gestión de incidentes de seguridad de la información. El personal necesita reconocer un incidente, saber qué hacer y comprender los beneficios del enfoque para la organización. Es necesario que la dirección apoye el esquema de gestión, para asegurar que la organización se comprometa con el suministro de recursos y mantenga una capacidad de respuesta a incidentes.

b) Actividad para actualizar las políticas de gestión del riesgo y de seguridad de la información, a nivel corporativo y a niveles de sistemas, redes y servicios específicos.

   Esto debería incluir referencia a la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Es necesario revisar regularmente las políticas en el contexto de la salida del esquema de gestión de incidentes de seguridad de la información (véase el numeral 5.3).

c) Actividad para definir y documentar un esquema detallado de gestión de incidentes de seguridad de la información. En general, la documentación del esquema debería abarcar los formularios, procedimientos, elementos organizacionales y herramientas de apoyo para la detección y reporte de evaluaciones y toma de decisiones relacionadas con incidentes de seguridad de la información, y las respuestas y aprendizaje de lecciones de estos incidentes. Los temas para incluir son:

   1) Una escala de clasificación de eventos/incidentes de seguridad de la información que se use para calificar los eventos/incidentes. En cualquier evento, la decisión se debería basar en los impactos adversos reales o proyectados, sobre las operaciones de los negocios de la organización.

      NOTA El Anexo C (informativo) presenta un ejemplo de enfoque para la categorización y la clasificación de eventos e incidentes de seguridad de la información.

   2) Los formatos de eventos/incidentes/vulnerabilidades de seguridad de la información:

- completados por la persona que reporta un evento de seguridad de la información (es decir, no es un miembro del equipo de gestión de incidentes de seguridad de la información), con la información grabada en una base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

- usados por el personal de gestión de incidentes de seguridad de la información, para construir sobre la información de eventos de seguridad de la información reportados inicialmente, y posibilitar un registro continuo de las evaluaciones de incidentes, entre otros, a través del tiempo, hasta que el incidente esté completamente solucionado. En cada etapa, la actualización se registra en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información. El registro completado de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información se usa entonces en actividades de resolución posteriores al incidente, y

- completados por la persona que reporta una vulnerabilidad de la seguridad de la información (que no ha sido aprovechada aún para causar un evento de seguridad de la información y posiblemente un incidente de seguridad de la información), con la información registrada en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Se recomienda que estos formatos sean electrónicos (por ejemplo, en una página web segura) que enlacen directamente con la base de datos electrónica de eventos/incidentes/vulnerabilidades de seguridad de la información. En el mundo de hoy, la operación de un esquema que utiliza papel sería muy dispendiosa. Sin embargo, puede ser necesario un esquema que utilice papel en donde no es posible usar un esquema electrónico.

NOTA En el Anexo D (informativo) se presentan ejemplos de formatos.

3) Las acciones y procedimientos documentados relacionados con el uso de formatos, es decir, asociados con detección de eventos, incidentes y vulnerabilidades de seguridad de la información, con enlaces a los procedimientos normales para el uso de copias de seguridad de datos y del sistema, servicio y/o red, y planes de gestión de crisis.

4) Los procedimientos operativos para el ISIRT, con procedimientos documentados y responsabilidades asociadas, y la asignación de roles a las personas designadas para llevar a cabo diversas actividades (un individuo puede estar asignado a más de un rol, dependiendo del tamaño, estructura y naturaleza del negocio de una organización), por ejemplo, que incluyan:

- apagar un sistema, servicio o red afectados, en determinadas circunstancias acordadas previamente con la gerencia de TI y/o del negocio pertinentes;

- dejar un sistema, servicio o red afectados, conectados y en funcionamiento;

- hacer seguimiento del flujo de datos desde un sistema, servicio o red afectada, hacia ellos o dentro de ellos;

- activar los procedimientos normales de respaldo y de gestión de crisis, y las acciones en línea con la política de seguridad del sistema, del servicio y/o de la red;

- hacer seguimiento y mantener en forma segura la evidencia electrónica en caso de que se requiera para un juicio legal o una acción disciplinaria interna, y

- comunicar detalles de incidentes de seguridad de la información a personal interno o externo a la organización.

En algunas organizaciones se puede hacer referencia al esquema como a un plan de respuesta a incidentes de seguridad de la información (véase el numeral 5.4).

d) Actividad para establecer el ISIRT, con un programa adecuado de formación diseñado, desarrollado y suministrado a su personal. De acuerdo con el tamaño, estructura y naturaleza del negocio, una organización puede tener un ISIRT conformado por un equipo dedicado, un equipo virtual o una combinación de las dos opciones. Un equipo dedicado puede tener miembros virtuales identificados en unidades/funciones específicas que deberían trabajar estrechamente con el ISIRT durante la resolución de un incidente de seguridad de la información (TIC, legal, relaciones públicas, compañías contratadas externamente, entre otros). Un equipo virtual puede tener un gerente de alto nivel que lidere el grupo, apoyado por grupos de individuos especializados en temas particulares, por ejemplo, en el manejo de ataques con códigos maliciosos, a quienes se llamará dependiendo del tipo de incidente involucrado (véase el numeral 5.5).

e) Actividad para establecer y preservar relaciones y conexiones adecuadas con organizaciones internas y externas que están directamente involucradas en la gestión de eventos, incidentes y vulnerabilidades.

f) Actividad para establecer, implementar y operar mecanismos técnicos y otro apoyo (incluido el organizacional) para brindar soporte al esquema de gestión de incidentes de seguridad de la información (y de esta manera al trabajo del ISIRT), con el fin de evitar la ocurrencia de incidentes de seguridad de la información o reducir la probabilidad de que ocurran (véase el numeral 5.6). Estos mecanismos pueden incluir los siguientes:

1) mecanismos internos de auditoría de seguridad de la información para evaluar el nivel de seguridad y hacer seguimiento a los sistemas vulnerables;

2) gestión de la vulnerabilidad (incluidas actualizaciones de seguridad y parches de seguridad de los sistemas vulnerables);

3) vigilancia tecnológica para detectar nuevos tipos de amenazas y ataques;

4) sistemas de detección de intrusión (para más detalles, véase la ISO/IEC 18043);

5) dispositivos de seguridad de redes, medios de protección y herramientas de seguimiento (para más detalles, véase la ISO/IEC 27033);

6) software anti-códigos maliciosos;

7) registros de auditoría, y software de seguimiento de registros y

8) responsabilidades y procedimientos de operación documentados para el equipo de soporte de operaciones.

g) actividad para diseñar y desarrollar un programa de formación y de toma de conciencia en gestión de eventos, incidentes y vulnerabilidades. Se debería informar a todo el personal de la organización, a través de sesiones informativas u otros mecanismos, acerca de la existencia de un esquema de gestión de eventos, incidentes y vulnerabilidades, sus beneficios y cómo reportar eventos e incidentes (y vulnerabilidades) de seguridad de la información. Paralelamente, se debería brindar formación adecuada al personal responsable de la gestión del esquema de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información, a las personas encargadas de la toma de decisiones involucradas en determinar si los eventos de seguridad de la información son incidentes, y a los individuos involucrados en la investigación de incidentes. Las sesiones informativas sobre toma de conciencia y las sesiones de formación, se deberían repetir posteriormente para tener en cuenta los cambios en el personal (véase el numeral 5.7).

h) Actividad para probar el uso del esquema de gestión de incidentes de seguridad de la información, sus procesos y procedimientos. Se deberían organizar pruebas periódicamente, no solo para poner a prueba el esquema en una situación real, sino también para verificar cómo se comporta el ISIRT bajo la presión de un incidente severo complejo. Se debería prestar atención particular a la creación de pruebas que se enfoquen en los escenarios de vulnerabilidades, amenazas y riesgos emergentes (véase el numeral 5.8). El esquema debería incluir estándares que apoyen la forma de intercambiar información, tanto dentro como fuera de la organización (si así lo exige la organización). Uno de los beneficios de intercambiar información es el conjunto de datos en métricas útiles para apoyar la toma de decisiones estratégicas del negocio. La membresía a una comunidad que comparte información de confianza también permite advertir, en forma temprana, acerca de ataques y se debería estimular en cualquier esquema y política asociada de gestión de incidentes de seguridad de la información.

Una vez finaliza esta fase, las organizaciones deberían estar completamente preparadas para gestionar adecuadamente los incidentes de seguridad de la información. Los siguientes numerales describen cada una de las actividades enumeradas arriba, incluido el contenido de cada documento requerido.

5.2 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.2.1 Introducción

Como parte de su política general del sistema de gestión de seguridad de la información (véase el numeral 4.2.1 b) de la norma NTC-ISO/IEC 27001:2005), o como parte de su política de seguridad de la información (véase el numeral 5.1.1 de la norma NTC- SO/IEC 27002:2005), una organización debería documentar su política para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información como un documento autónomo. El tamaño, estructura y naturaleza del negocio de una organización y el alcance de su programa de gestión de incidentes de seguridad de la información son factores decisivos para determinar qué opción adoptar. Cada organización debería dirigir su política de gestión de incidentes de seguridad de la información a todas las personas que tienen acceso legítimo a sus sistemas de información e instalaciones relacionadas.

Antes de formular la política, la organización debería llevar a cabo una revisión de la seguridad de la información en la que se destaquen sus vulnerabilidades, confirmación de la necesidad de gestionar los incidentes de seguridad de la información, y de la identificación de los beneficios para la organización entera y para sus áreas.

5.2.2 Partes involucradas

Una organización debería asegurar que su política de gestión de incidentes de seguridad de la información sea aprobada por un alto directivo de la organización, con el compromiso y el aval documentados de toda la alta dirección. Ésta política se debería poner a disposición de todos los empleados y contratistas, y se debería tener en cuenta en las sesiones de concientización y formación en seguridad de la información (véase el numeral 5.7).

5.2.3 Contenido

La organización debería asegurar que el contenido de su política de gestión de incidentes de seguridad de la información tenga en cuenta los siguientes temas:

a) La importancia que tiene para la organización la gestión de incidentes de seguridad de la información, el compromiso de la alta dirección con ella, y el esquema relacionado.

b) Una visión general sobre la detección de eventos de seguridad de la información, reporte y recolección de la información pertinente, y cómo se debería usar esta información para determinar los incidentes de seguridad de la información.

   Esta visión general debería incluir un resumen de los tipos posibles de eventos de seguridad de la información, cómo reportarlos, qué reportar, en dónde y a quién, y cómo manejar los nuevos tipos de eventos de seguridad de la información. También debería incluir un resumen de reportes y manejo de vulnerabilidades de seguridad de la información.

c) Una visión general de la evaluación de incidentes de seguridad de la información, que incluya un resumen de quién es el responsable, qué se debe hacer, notificación y escalamiento.

d) Un resumen de las actividades posteriores a la confirmación de que un evento de seguridad de la información es un incidente de seguridad de la información.

e) Una referencia a la necesidad de asegurar que todas las actividades de gestión de incidentes de seguridad de la información se registren adecuadamente para un análisis posterior y que se lleve a cabo seguimiento continuo, para asegurar la preservación segura de la evidencia electrónica, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas.

f) Las actividades posteriores a la resolución de incidentes de seguridad de la información, donde se incluya el aprendizaje, a partir del proceso y la mejora de dicho proceso, después de los incidentes de seguridad de la información.

g) Una visión general del reporte y manejo de las vulnerabilidades de seguridad de la información.

h) Detalles de dónde se mantiene la documentación del esquema, incluidos los procedimientos.

i) Una visión general del ISIRT, que abarque los siguientes temas.

1. La estructura organizacional del ISIRT y la identificación del líder del ISIRT y otro personal clave, incluidos los responsables de:

- informar a la alta dirección acerca de los incidentes,
- hacerse cargo de las investigaciones y promover el seguimiento, entre otros
- el enlace con las organizaciones externas (cuando es necesario).

2) El documento de gestión de la seguridad de la información, que especifica qué hará el ISIRT y bajo qué autoridad funcionará. Éste, como mínimo, debería incluir una declaración de la misión, una definición del alcance del ISIRT, y los detalles del patrocinador (*sponsor*) de la alta dirección

3) La declaración de la misión de ISIRT que se enfoca en las actividades esenciales del equipo. Para ser considerado como un ISIRT, el equipo debería apoyar la evaluación, respuesta y gestión de incidentes de seguridad de la información, para obtener una conclusión exitosa. Las metas y propósitos del equipo son especialmente importantes y requieren una definición clara e inequívoca.

4) Una definición del alcance de las actividades del ISIRT. Normalmente, el alcance del ISIRT de una organización comprende todos los sistemas, servicios y redes de información de la organización. En otros casos, una organización puede, por cualquier razón, solicitar que el alcance sea inferior a ese, en cuyo caso se debe documentar claramente lo que el alcance incluye y lo que no incluye.

5) La identificación de un alto directivo, un miembro del consejo o director ejecutivo que tenga la autoridad para tomar decisiones sobre el ISIRT y también establecer los niveles de autoridad para éste; saber esto ayuda al personal de la organización a entender la información básica y organización del ISIRT, y es una información vital para construir confianza en éste. Sin embargo, es necesario tener en cuenta que antes de que se publique este detalle, se debería examinar desde una perspectiva legal. En algunas circunstancias, la divulgación de la autoridad de un equipo puede exponer éste a reclamos por responsabilidad civil.

6) Enlaces a organizaciones que brindan apoyo externo específico, tales como equipos forenses (véase el numeral 5.5.4).

j) Una visión general de los mecanismos técnicos y otros mecanismos de apoyo.

k) Una visión general del programa de formación y toma de conciencia sobre la gestión de incidentes de seguridad de la información.

l) Un resumen de los aspectos legales y reglamentarios que se deben tener en cuenta (para más detalles, consulte el Anexo E (Informativo)).

5.3 INTEGRACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN CON OTRAS POLÍTICAS

5.3.1 Introducción

Una organización debería incluir contenido de la gestión de incidentes en sus políticas corporativas de gestión del riesgo y de seguridad de la información, al igual que a niveles específicos de sistemas, servicios y redes, y relacionar su contenido con la política de gestión de incidentes. La integración debería estar dirigida a lo siguiente:

a) Describir por qué es importante la gestión de incidentes de seguridad de la información, particularmente un esquema de manejo y reporte de incidentes de seguridad de la información.

b) Indicar el compromiso de la alta dirección con la necesidad de una preparación y respuesta adecuadas a incidentes de seguridad de la información, es decir, con el esquema de gestión de incidentes de seguridad de la información.

c) Asegurar consistencia entre las diversas políticas.

d) Asegurar respuestas planificadas, sistemáticas y serenas ante incidentes de seguridad de la información, para minimizar de esta manera los impactos adversos de los incidentes.

Para orientación sobre la evaluación y la gestión de evaluación de riesgos de seguridad de la información, véase la NTC- ISO/IEC 27005:2008.

5.3.2 Contenido

Cada organización debería actualizar y mantener sus políticas corporativas de gestión del riesgo, de seguridad de la información, y las políticas específicas de seguridad de la información de sistemas, servicios o redes. Estas políticas necesitan hacer referencia a una política corporativa de gestión de incidentes de seguridad de la información, y explícitamente, a un esquema asociado.

a) Las secciones relacionadas deberían hacer referencia al compromiso de la alta dirección.

b) Las secciones relacionadas deberían delinear la política.

c) Las secciones relacionadas deberían explicar los procesos del esquema, y la infraestructura relacionada.

d) Las secciones pertinentes deberían explicar los requisitos para detectar, reportar, evaluar y gestionar eventos, incidentes y vulnerabilidades de seguridad de la información.

e) Las secciones pertinentes deberían indicar claramente el personal responsable de autorizar y/o emprender determinadas acciones críticas (por ejemplo, desconectar un sistema de información, o incluso apagarlo).

Las políticas deberían incluir el requisito de que es necesario establecer mecanismos de revisión adecuados. Estos mecanismos necesitan asegurar que la información obtenida de la detección, seguimiento y resolución de incidentes de seguridad de la información y de tratar las

vulnerabilidades de seguridad de la información reportadas se use como entrada para asegurar la eficacia continua de las políticas corporativas de gestión del riesgo y de seguridad de la información, y las políticas de seguridad de la información de redes, servicios y sistemas específicos.

5.4 ESQUEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.4.1 Introducción

El objetivo del esquema de gestión de incidentes de seguridad de la información es brindar documentación detallada que describa las actividades y procedimientos para tratar los eventos e incidentes de seguridad de la información, y comunicar estos eventos, incidentes y vulnerabilidades. El esquema de gestión de incidentes de seguridad de la información entra en vigor, siempre que se detecte un evento de seguridad de la información, o que se reporte una vulnerabilidad de la seguridad de la información. Cada organización debería usar el esquema como una guía para:

a) responder a eventos de seguridad de la información;

b) determinar si los eventos de seguridad de la información llegan a ser incidentes de seguridad de la información;

c) gestionar incidentes de seguridad de la información hasta su conclusión;

d) responder a vulnerabilidades de seguridad de la información;

e) identificar las lecciones aprendidas y cualquier mejora al esquema y/o seguridad en general que se requiera, y

f) hacer las mejoras identificadas.

5.4.2 Partes involucradas

Una organización debería asegurar que el esquema de gestión de incidentes de seguridad de la información esté dirigido a todo el personal y a los contratistas asociados, proveedores de servicios de TIC, proveedores de telecomunicaciones y compañías de contratación externa, de manera que se abarquen las siguientes responsabilidades:

a) detectar y reportar eventos de seguridad de la información (ésta es responsabilidad de cualquier personal ya sea contratado o permanente en una organización y sus compañías);

b) evaluar y responder a eventos e incidentes de seguridad de la información, involucrarse en actividades de aprendizaje posteriores a la resolución de incidentes, y mejorar la seguridad de la información y el propio esquema de gestión de incidentes de seguridad de la información (esta es responsabilidad de los miembros del PoC (Punto de Contacto), el ISIRT, la dirección, el personal de relaciones públicas y los representantes legales), y

c) reportar vulnerabilidades de seguridad de la información (ésta es responsabilidad de cualquier personal ya sea contratado o permanente en una organización y sus compañías), y tratarlas.

El esquema también debería tener en cuenta a cualquier usuario de terceras partes, los incidentes de seguridad de la información y las vulnerabilidades asociadas reportadas por organizaciones externas y organizaciones gubernamentales y comerciales de suministro de información de vulnerabilidades e incidentes de seguridad.

5.4.3 Contenido

Cada organización debería asegurar que el contenido de la documentación de su esquema de gestión de incidentes de seguridad de la información incluya lo siguiente:

a) Una visión general de la política de gestión de incidentes de seguridad de la información.

b) Una visión general de todo el esquema de gestión de incidentes de seguridad de la información.

c) Las actividades, procedimientos e información detallados asociados con lo siguiente:

   1) Planificación y preparación de

      i) Un enfoque normalizado para la categorización y la clasificación de eventos/incidentes de seguridad de la información, para posibilitar el suministro de resultados consistentes. En cualquier evento, la decisión se debería basar en los impactos adversos reales o proyectados, sobre las operaciones de los negocios de la organización, y la orientación asociada.

         NOTA El Anexo C (Informativo) presenta un ejemplo de enfoque para la categorización y clasificación de eventos e incidentes de seguridad de la información.

      ii) Una estructura en forma de base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información normalizada, que es probable que brinde la capacidad para comparar resultados, mejorar la información de alertas y posibilitar una visión más exacta de las amenazas y las vulnerabilidades de los sistemas de información.

      iii) Orientación para decidir si se requiere escalar el asunto durante cada proceso pertinente, y a quién, y los procedimientos asociados. Con base en la orientación proporcionada en la documentación del esquema de gestión de incidentes, cualquiera que evalúe un evento, incidente o vulnerabilidad de seguridad de la información debería saber en qué circunstancias es necesario escalar los asuntos, y a quién se deberían escalar. Además, puede haber circunstancias no previstas en que esto puede ser necesario. Por ejemplo, un incidente menor de seguridad de la información podría evolucionar a una situación significativa o de crisis, si no se maneja adecuadamente, o un incidente menor de seguridad de la información al que se no se hace seguimiento en una semana se puede convertir en un incidente mayor de seguridad de la información. La orientación debería definir los tipos de eventos e incidentes de seguridad de la información, las formas de escalarlos, y quién puede iniciar la acción de escalarlos.

iv) Los procedimientos que se deben seguir para asegurar que todas las actividades de gestión de incidentes de seguridad de la información se registren adecuadamente en el formato adecuado, y que el análisis de los registros lo lleve a cabo el personal designado.

v) Los procedimientos y mecanismos para asegurar que el régimen de control de cambios se mantenga y cubra el seguimiento de los eventos, incidentes y vulnerabilidades de seguridad de la información y las actualizaciones de reportes de eventos/incidentes/vulnerabilidades de seguridad de la información y las actualizaciones del propio esquema.

vi) Los procedimientos para análisis forense de seguridad de la información.

vii) Los procedimientos y orientación sobre el uso de Sistemas de Detección de Intrusión (SDI), asegurando que se hayan tratado los aspectos legales y reglamentarios asociados. La orientación debería incluir la discusión de las ventajas y desventajas de emprender actividades de vigilancia de atacantes. La norma ISO/IEC 18043:2006 presenta más información sobre el SDI.

viii) La orientación y los procedimientos asociados con los mecanismos técnicos y organizacionales que se establezcan, implementen y operen para impedir la ocurrencia de incidentes de seguridad de la información y reducir la probabilidad de ocurrencia de incidentes de seguridad de la información, y tratar los incidentes de seguridad de la información ocurridos.

ix) El material para el programa de formación y de toma de conciencia en gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

x) Los procedimientos y especificaciones para poner a prueba el esquema de gestión de incidentes de seguridad de la información.

xi) El esquema de la estructura organizacional para la gestión de incidentes de seguridad de la información.

xii) Los términos de referencia y responsabilidades del ISIRT en conjunto, o de los miembros individuales.

xiii) La información de contacto importante.

2) Detección y reporte

i) Detectar y reportar la ocurrencia de eventos de seguridad de la información (por medios humanos o automáticos).

ii) Recolectar la información sobre eventos de seguridad de la información.

iii) Detectar y reportar vulnerabilidades de seguridad de la información.

iv) Registrar completamente toda la información recolectada en la base de datos de gestión de incidentes de seguridad de la información.

3) Evaluación y decisión

i) El PoC (Punto de Contacto) que lleva a cabo evaluaciones de eventos de seguridad de la información (incluido escalar el asunto) usando la escala acordada de clasificación de eventos/incidentes de seguridad de la información (incluida la determinación del impacto de los eventos con base en los activos/servicios afectados) y que decide si los eventos se deberían clasificar como incidentes de seguridad de la información.

ii) El ISIRT que evalúa los eventos de seguridad de la información debería confirmar si un evento es un incidente de seguridad de la información o no, y luego se debería llevar a cabo otra evaluación usando la escala de clasificación acordada para incidentes/eventos de seguridad de la información, para confirmar los detalles del tipo de evento (incidente potencial) y recurso afectado (categorización). A continuación, se deberían tomar las decisiones acerca de cómo se debería tratar el incidente de seguridad de la información confirmado, por quién y con qué prioridad, al igual que los niveles de escalamiento.

iii) Evaluar las vulnerabilidades de la seguridad de la información (que aún no han sido aprovechadas para causar eventos de seguridad de la información e incidentes potenciales de seguridad de la información), y tomar decisiones acerca de cuál necesita tratarse, quién lo va a tratar, cómo y con qué prioridad.

iv) Registrar completamente todos los resultados de la evaluación y decisiones relacionadas en la base de datos de gestión de incidentes de seguridad de la información.

4) Respuestas

i) El ISIRT realiza una revisión para determinar si el incidente de seguridad de la información está bajo control, y

- si el incidente está bajo control, instigar la respuesta requerida, ya sea en forma inmediata (en tiempo real o cerca a él) o posteriormente;

- si el incidente no está bajo control, o va a haber impacto severo en los servicios esenciales de la organización, instigar actividades de manejo de crisis, llevando el asunto a la función de manejo de crisis.

ii) Definir un mapa de todas las funciones y organizaciones internas y externas que se deberían involucrar durante la gestión de un incidente.

iii) Llevar a cabo el análisis forense de seguridad de la información, según se requiera.

iv) Escalar el asunto, según se requiera.

v) Asegurar que todas las actividades involucradas se registren adecuadamente para su posterior análisis.

vi) Asegurar que se recolecte evidencia electrónica y que se almacene en forma segura.

vii) Asegurar que se mantenga el régimen de control de cambios, y en consecuencia que la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información se mantenga actualizada.

viii) Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, a otro personal interno o externo a la organización.

ix) Tratar las vulnerabilidades de seguridad de la información.

x) Una vez que el incidente se ha tratado exitosamente, cerrarlo formalmente y registrar esto en la base de datos de gestión de incidentes de seguridad de la información.

Cada organización debería asegurar que la documentación del esquema de gestión de incidentes de seguridad de la información prevea respuesta a estos incidentes, tanto en forma inmediata como a largo plazo. Todos los incidentes de seguridad de la información deberían someterse a una evaluación temprana de los impactos potenciales adversos en las operaciones del negocio, tanto a corto como a largo plazo (por ejemplo, un desastre grave puede ocurrir algún tiempo después de un incidente inicial de seguridad de la información). Además, debería prever algunas respuestas necesarias para incidentes de seguridad de la información completamente imprevistos, donde se requieren controles *ad hoc*. Incluso para esta situación, las organizaciones deberían abarcar las directrices generales en la documentación del esquema acerca de los pasos que pueden ser necesarios.

5) Lecciones aprendidas

i) Llevar a cabo el análisis forense de seguridad de la información, según se requiera.

ii) Identificar las lecciones aprendidas de los incidentes y vulnerabilidades de seguridad de la información.

iii) Revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información (controles nuevos y/o actualizados), al igual que la política de gestión de incidentes de seguridad de la información, como resultado de las lecciones aprendidas.

iv) Revisar, identificar, y si es posible, hacer mejoras a los resultados de la revisión por la dirección y la evaluación de riesgos para la seguridad de la información existentes, como resultado de las lecciones aprendidas.

v) Revisar cómo fue la eficacia de los procesos, los procedimientos, los formatos de reporte y/o la estructura organizacional para responder a la evaluación y la recuperación de cada incidente de seguridad de la información y tratar las vulnerabilidades de seguridad de la información, y con base en las lecciones aprendidas identificar y hacer mejoras en el

esquema de gestión de incidentes de seguridad de la información y su documentación.

vi) Actualizar la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

vii) Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si la organización lo desea).

5.4.4 Procedimientos

Antes de comenzar la operación del esquema de gestión de incidentes de seguridad de la información es importante que una organización haya documentado y verificado que los procedimientos están disponibles. Cada procedimiento debería indicar aquellos grupos o individuos responsables de su uso y gestión, según sea adecuado, del PoC (Punto de Contacto) y/o del ISIRT. Estos procedimientos deberían asegurar que se recolecta y almacena evidencia electrónica en forma segura, y que se hace seguimiento continuo a su preservación segura, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas. Además, debería haber procedimientos documentados que abarquen no solamente las actividades del PoC (Punto de Contacto) y del ISIRT, sino también las involucradas con el análisis forense de seguridad de la información y las actividades durante la crisis, si no se tratan en otra parte, por ejemplo, en el plan de continuidad del negocio o en el plan de gestión de crisis. Los procedimientos documentados deberían estar en línea completamente con la política documentada de gestión de incidentes de seguridad de la información y otra documentación del esquema de gestión de seguridad de incidentes de información.

Es importante entender que no todos los procedimientos necesitan estar disponibles al público. Por ejemplo, no es necesario que todo el personal de la organización entienda la operación interna de un ISIRT para poder interactuar con él. El ISIRT debería asegurar que la orientación disponible públicamente, incluida la información resultante del análisis de incidentes de seguridad de la información, esté en un formato fácilmente disponible, por ejemplo, en la intranet de la organización. También puede ser importante mantener controlados algunos detalles del esquema de gestión de incidentes de seguridad de la información para evitar que alguna persona con acceso a información confidencial altere el proceso de investigación. Por ejemplo, si un funcionario de un banco que está haciendo malversación de fondos tiene conocimiento de algunos detalles del esquema, puede estar en capacidad de ocultar sus actividades a los investigadores o entorpecer la detección, la investigación y la recuperación de un incidente de seguridad de la información.

El contenido de los procedimientos operativos depende de varios criterios que se relacionan, especialmente con la naturaleza de los eventos, incidentes y vulnerabilidades potenciales de seguridad de la información, y con los tipos de activos de sistemas de información que podrían estar involucrados y sus entornos. De esta manera, un procedimiento operativo puede estar relacionado con un tipo particular de incidente o producto (por ejemplo, *firewalls*, bases de datos, sistemas operativos, aplicaciones) o con un producto específico. Cada procedimiento operativo debería identificar claramente los pasos a seguir, y quién debe hacerlo. Debería reflejar la experiencia de las fuentes externas (por ejemplo, los ISIRT gubernamentales o comerciales, o similares y los proveedores) al igual que las fuentes internas.

Debería haber procedimientos operativos para tratar los tipos de eventos, incidentes y vulnerabilidades de seguridad de la información que ya se conocen. Debería haber además, procedimientos operativos que se han de seguir para cuando un evento, incidente o vulnerabilidad identificados de la seguridad de la información no sean de ningún tipo conocido. En este caso, se debería tener en cuenta lo siguiente:

a) El proceso de reporte para el manejo de estas excepciones.

b) La orientación acerca del momento oportuno para obtener la aprobación de la dirección para evitar cualquier retraso en la respuesta.

c) La delegación autorizada previamente, de la toma de decisiones sin el proceso de aprobación normal.

5.4.5 Confianza

El ISIRT desempeña un papel crucial en la seguridad general de la información de una organización El ISIRT requiere la colaboración de todo el personal de la organización para detectar, resolver e investigar incidentes de seguridad de la información. Es fundamental que el ISIRT cuente con la confianza de todos, tanto interna como externamente. La adopción del anonimato para el reporte de vulnerabilidades eventos e incidentes puede ser útil para construir confianza.

Una organización debería asegurar que su esquema de gestión de incidentes de seguridad de la información aborda situaciones en las que es importante asegurar el anonimato de la parte o persona que reporta los incidentes o vulnerabilidades potenciales de seguridad de la información bajo circunstancias específicas. Cada organización debería contar con disposiciones que ilustren claramente la expectativa de anonimato o la falta de éste, para las personas o partes que reportan un incidente o vulnerabilidad potencial de seguridad de la información. El ISIRT puede necesitar obtener información adicional no transmitida inicialmente por la persona o parte que reportó el incidente. Además, se puede obtener información importante sobre el propio incidente o vulnerabilidad de seguridad de la información, de quien lo detectó primero.

Otro enfoque que puede adoptar el ISIRT es ganarse la confianza de los usuarios, por medio de procesos transparentes y maduros. El ISIRT debería trabajar para educar a los usuarios, explicar cómo funciona, cómo protege la confidencialidad de la información recolectada, y cómo maneja los reportes de eventos, incidentes y vulnerabilidades de los usuarios.

El ISIRT debería tener capacidad de satisfacer eficientemente las necesidades funcionales, financieras, legales y políticas de la organización y debería estar en capacidad de ejercer discreción organizacional, cuando se gestionen incidentes y vulnerabilidades de seguridad de la información. La función del ISIRT también se debería auditar independientemente para confirmar que todos los requisitos del negocio se satisfagan eficazmente.

Además, una buena forma de lograr otro aspecto de independencia es separar la cadena de reporte de incidentes y vulnerabilidades desde la gerencia en línea operativa, y hacer que un gerente de alto nivel sea el responsable directo de la gestión de respuestas de incidentes y vulnerabilidades. Los recursos financieros de la capacidad también se deberían separar para evitar influencia indebida.

5.4.6 Confidencialidad

Un esquema de gestión de incidentes de seguridad de la información puede contener información confidencial y se puede requerir que las personas involucradas en tratar incidentes y vulnerabilidades manejen información confidencial. Una organización debería asegurar que se establezcan los procesos necesarios para anonimizar la información confidencial y requerir que las personas con acceso a información confidencial firmen acuerdos de confidencialidad. Si los eventos/incidentes/vulnerabilidades se registran, por medio de un sistema de gestión de problemas generalizado, es posible que se tengan que omitir los detalles confidenciales.

Adicionalmente, una organización debería asegurar que el esquema de gestión de incidentes de seguridad de la información prevea que se controle la comunicación de incidentes y vulnerabilidades a partes externas, incluidos los medios, socios comerciales, clientes, organizaciones que velan por el cumplimiento de las leyes, y el público en general.

5.5 ESTABLECIMIENTO DEL ISIRT

5.5.1 Introducción

El objetivo de establecer el ISIRT es proveer a la organización con una capacidad adecuada para evaluar, responder a los incidentes de seguridad de la información, aprender de ellos, y brindar la coordinación, gestión, retroalimentación y comunicación necesarias. Un ISIRT contribuye a la reducción de daño económico y físico, al igual que la reducción de daño para la reputación de las organizaciones, que algunas veces se asocia con incidentes de seguridad de la información.

5.5.2 Miembros y estructura

El tamaño, estructura y composición del ISIRT deberían ser adecuados al tamaño, estructura y naturaleza del negocio de la organización. Aunque el ISIRT puede constituir un equipo o departamento aislado, los miembros pueden compartir otros deberes, lo cual estimula los aportes de miembros de una variedad de áreas dentro de la organización. Una organización debería evaluar si requiere un equipo dedicado, un equipo virtual o una combinación de los dos. El número de incidentes y las actividades realizadas por el ISIRT deberían orientar a la organización en su selección.

El ISIRT pasa por diferentes etapas de madurez y con frecuencia se adoptan ajustes al modelo organizacional, con base en el escenario específico que enfrenta la organización. Siempre que se justifique, se recomienda que haya un equipo permanente liderado por un gerente de alto nivel. Los equipos ISIRT virtuales pueden ser liderados por un gerente de alto nivel. Éste debería estar apoyado por individuos especializados en temas particulares, por ejemplo, el manejo de ataques de códigos maliciosos, a quienes se convoca dependiendo del tipo de incidente de seguridad de la información involucrado. Dependiendo del tamaño, estructura y naturaleza del negocio de una organización, un miembro también puede desempeñar más de un rol dentro del ISIRT. El ISIRT puede tener individuos de diferentes partes de la organización (por ejemplo, operaciones comerciales, TIC, auditorías, recursos humanos y mercadeo). Esto también se aplica en ISIRT permanentes, en donde, incluso el personal dedicado requiere el apoyo de otros departamentos.

Los miembros del equipo deberían ser accesibles, de manera que sus nombres y los detalles de contacto de cada miembro y sus miembros de respaldo estén disponibles dentro de la organización. Los detalles necesarios se deberían indicar claramente en la documentación del esquema de gestión de incidentes de seguridad de la información, incluidos los documentos de procedimiento, y los formatos de reporte, pero no en las declaraciones de la política.

El líder del ISIRT usualmente debería tener una línea de reporte a la alta gerencia, separada de las operaciones normales del negocio. Se le debería delegar autoridad para tomar decisiones inmediatas acerca de cómo tratar un incidente, y se debería asegurar de que todos los miembros del ISIRT tengan los niveles de conocimiento y habilidades requeridas, y que se mantengan. El líder del ISIRT debería asignar la investigación de cada incidente al miembro más adecuado de su equipo, y a cada incidente se le debería asignar un líder.

5.5.3 Relación con otras partes de la organización

El ISIRT debería tener la responsabilidad de asegurar que se resuelvan los incidentes, y en este contexto, el líder del ISIRT y los miembros de su equipo deberían tener un grado de autoridad para tomar las acciones necesarias consideradas adecuadas para responder a incidentes de seguridad de la información. Sin embargo, las acciones que puedan tener efectos adversos en toda la organización, ya sea financieramente o en términos de reputación, se deberían acordar con la alta gerencia. Por esta razón, es esencial que el esquema y la política de gestión de incidentes de seguridad de la información presenten en detalle la autoridad pertinente a la cual el líder del ISIRT reporta los incidentes graves de seguridad de la información.

Los procedimientos y responsabilidades para tratar con los medios también se deberían acordar con la alta dirección y se deberían documentar. Estos procedimientos deberían especificar quién en la organización trata las consultas de los medios, y como esta parte de la organización interactúa con el ISIRT.

5.5.4 Relación con las partes externas interesadas

Las organizaciones deberían establecer relaciones entre el ISIRT y las partes externas interesadas adecuadas. Estas partes externas interesadas pueden incluir las siguientes:

a) personal de soporte contratado externamente,

b) ISIRT de organizaciones externas,

c) proveedores de servicios gestionados, incluidos proveedores de servicios de telecomunicaciones, PSI (Proveedores de Servicios de Internet) y proveedores,

d) organizaciones que velan por el cumplimiento de la ley,

e) autoridades de emergencias,

f) organizaciones gubernamentales pertinentes,

g) personal legal,

h) funcionarios de relaciones públicas o miembros de los medios, o ambos,

i) socios del negocio,

j) clientes, y

k) el público en general.

5.6 SOPORTE TÉCNICO Y OTRO (incluido el soporte operativo)

Para asegurar que se puedan dar respuestas rápidas y eficaces a los incidentes de seguridad de la información, las organizaciones deberían adquirir, preparar y poner a prueba todos los medios técnicos y otros medios de soporte necesarios. Esto incluye lo siguiente:

a) acceso a detalles de los activos de la organización, con un registro actualizado de los mismos, e información sobre las relaciones con las funciones del negocio,

b) acceso a procedimientos documentados relacionados con la gestión de crisis,

c) procesos de comunicaciones documentados y promulgados,

d) uso de una base de datos de eventos/eventos/incidentes de seguridad de la información y los medios técnicos para alimentar y actualizar la base rápidamente, analizar su información y facilitar las respuestas (en algunos casos la organización puede solicitar registros manuales) con la base de datos mantenida en forma segura,

e) medios para la recolección y el análisis de evidencia forense de seguridad de la información, y

f) disposiciones adecuadas para gestión de crisis para la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información (para orientación sobre gestión de la continuidad del negocio, véase la ISO/IEC 27031).

Una organización se debería asegurar de que los medios técnicos usados para alimentar y actualizar rápidamente la base de datos, analizar su información y facilitar las respuestas a los incidentes de seguridad de la información, brinden soporte a lo siguiente:

g) la rápida adquisición de reportes de eventos/incidentes/vulnerabilidades de seguridad de la información,

h) notificación de personal externo previamente seleccionado, por medios adecuados (por ejemplo, correo electrónico, fax o teléfono), para lo cual se requiere el mantenimiento de una base de datos de contactos fácilmente accesible (incluidas copias en papel y otras copias de respaldo) y la facilidad para transmitir información a individuos, de forma segura, cuando sea pertinente,

i) precauciones proporcionales a los riesgos evaluados, para asegurar que las comunicaciones electrónicas, ya sean por Internet o no, no puedan ser interceptadas y permanezcan disponibles mientras el sistema, el servicio y/o la red están bajo ataque (esto puede requerir que se implementen mecanismos de comunicaciones alternativas planificados previamente),

j) asegurar la recolección de todos los datos acerca del sistema, servicio y/o red de información y todos los datos procesados.

k) usar el control de integridad criptográfica para ayudar a determinar si el sistema, servicio y/o red, y qué partes de éstos, y qué datos, fueron cambiados, si son proporcionales a los riesgos evaluados,

l) facilitar el archivo y la seguridad de la información recolectada (por ejemplo, colocando firmas digitales a los registros, y otra evidencia antes de almacenamiento fuera de línea en medios de lectura únicamente, tales como CD o DVD ROM),

m) posibilitar la preparación de impresiones (por ejemplo, de los registros), incluidos los que presentan el avance de un incidente, el proceso de resolución y la cadena de custodia,

n) llevar el sistema, servicio y/o red de información a operación normal, con los siguientes procedimientos que están en línea con la gestión de crisis pertinente:

    1) pruebas de las copias de respaldo,

2) control de códigos maliciosos,

3) medios originales con software de sistemas y de aplicaciones,

4) medios de arranque, y

5) parches para sistemas y aplicaciones, limpios, confiables y actualizados.

Cada vez es más común que las organizaciones creen una imagen de base estándar a partir de los medios de instalación y que usen esta imagen como una base limpia para crear sistemas. Con frecuencia es preferible el uso de esta imagen, en lugar de los medios originales, ya que la imagen ya ha sido corregida, endurecida, probada, etc.

Es posible que un sistema, servicio o red de información atacada no funcione correctamente. Por tanto, en la medida de lo posible, ningún medio técnico (software y hardware) necesario para responder a un incidente de seguridad de la información debería depender de los "principales" sistemas, servicios y/o redes de la organización para sus operaciones, proporcionalmente a los riesgos evaluados. Todos los medios técnicos se deberían seleccionar cuidadosamente, implementar correctamente y someter a prueba, en forma regular (incluida la prueba de las copias de respaldo). Si es posible, los medios técnicos deberían ser completamente independientes.

NOTA Los medios técnicos descritos en este numeral no incluyen los medios técnicos usados para detectar incidentes e intrusiones de seguridad de la información directamente y para notificar automáticamente a las personas adecuadas. En la norma ISO/IEC 18043 se describen estos medios técnicos.

Aunque el PoC (Punto de Contacto) de la organización tiene un rol regular más amplio, para brindar soporte a todos los aspectos de TI y manejo de la información relacionada, tiene un rol clave en la gestión de incidentes de seguridad de la información. Cuando los eventos de seguridad de la información se reportan por primera vez, el PoC (Punto de Contacto) los trata en la fase de detección y reporte. El PoC (Punto de Contacto) debería examinar la información recolectada y hacer una evaluación inicial para determinar si los eventos se deberían clasificar o no como incidentes. Si el evento no se clasifica como un incidente, el PoC (Punto de Contacto) debería tratarlo como evento. Si un evento se clasifica como incidente, es posible que lo trate el PC, aunque se espera que en la mayoría de casos sea necesario pasar al ISIRT la responsabilidad de tratar los incidentes. No se espera que el personal del PoC (Punto de Contacto) sea experto en seguridad.

5.7 TOMA DE CONCIENCIA Y FORMACIÓN

La gestión de incidentes de seguridad de la información es un proceso que involucra no solamente medios técnicos, sino también personas. Por tanto, debería contar con el soporte de individuos con conocimiento y formación adecuada en seguridad de la información, dentro de la organización.

La toma de conciencia y la participación de todo el personal de la organización son cruciales para el éxito de un enfoque estructurado, para la gestión de incidentes de seguridad de la información. Aunque se debería solicitar la participación de los usuarios, es menos probable que participen eficazmente en su operación, si desconocen cómo ellos y su departamento se pueden beneficiar de participar en un enfoque estructurado para la gestión de incidentes de seguridad de la información. Además, la eficiencia y la calidad operativa de un enfoque estructurado para la gestión de incidentes de seguridad de la información dependen de muchos factores, entre ellos, la obligación de notificar incidentes, la calidad de la notificación, la facilidad de uso, la rapidez y la formación. Algunos de estos factores están relacionados con

asegurarse de que los usuarios son conscientes del valor de la gestión de incidentes de seguridad de la información y están motivados a reportar incidentes.

La organización debería asegurar que el rol de gestión de incidentes de seguridad de la información se promueva activamente, como parte del programa corporativo de formación y toma de conciencia de seguridad de la información. El programa de toma de conciencia y el material relacionado deberían estar a disposición de todo el personal, incluidos los empleados nuevos, los usuarios y los contratistas por tercera parte, según sea pertinente y debería haber un programa de formación específico para el PoC, los miembros del ISIRT, el personal y los administradores específicos de seguridad de la información, según sea necesario. Cada grupo de personas involucradas directamente en la gestión de incidentes puede necesitar diferentes niveles de formación, dependiendo del tipo, frecuencia y carácter crítico de su interacción con el esquema de gestión de incidentes de seguridad de la información.

Las instrucciones sobre toma de conciencia de la organización deberían incluir lo siguiente:

a) los beneficios que se obtendrán del enfoque estructurado para la gestión de incidentes de seguridad de la información, tanto para la organización como para su personal;

b) cómo funciona el esquema de gestión de incidentes de seguridad de la información, incluido su alcance y el flujo de trabajo de gestión de eventos, incidentes y vulnerabilidades de seguridad;

c) cómo reportar sobre eventos, incidentes y vulnerabilidades de seguridad de la información;

d) información que se mantiene de incidentes, y las salidas de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información;

e) controles sobre la confidencialidad de las fuentes, según sea pertinente;

f) acuerdos de niveles de servicio del esquema;

g) notificación de resultados: bajo qué circunstancias se recomiendan las fuentes;

h) cualquier restricción impuesta por acuerdos de no divulgación;

i) la autoridad de la organización para gestión de incidentes de seguridad de la información y su línea de reporte, y

j) quién recibe los reportes del esquema de gestión de incidentes de seguridad de la información, y cómo se distribuyen.

En algunos casos, puede ser recomendable que la organización incluya en otros programas de formación (por ejemplo, programas de orientación del personal o programas corporativos generales de toma de conciencia sobre seguridad) detalles sobre toma de conciencia, específicamente acerca de incidentes de seguridad de la información. Este enfoque de toma de conciencia puede brindar un contexto valioso pertinente para grupos particulares de personas, y mejora la eficacia y la eficiencia del programa de formación.

Antes de que el esquema de gestión de incidentes de seguridad de la información se haga operativo, la organización debería asegurar que el personal pertinente esté familiarizado con los procedimientos involucrados en la detección y reporte de eventos de seguridad de la información, y que el personal seleccionado esté muy familiarizado con las actividades

posteriores. Esto se debería complementar con instrucciones y cursos de formación regulares en toma de conciencia. La formación debería ir apoyada en ejercicios específicos y pruebas a los miembros del PoC (Punto de Contacto), el ISIRT, y al personal y a los administradores específicos de seguridad de la información.

Además, los programas de toma de conciencia y formación deberían ir complementados por el establecimiento y la operaciones de soporte, mediante una "línea de emergencia" del personal de gestión de incidentes de seguridad de la información, para minimizar retrasos en el reporte y manejo de eventos, incidentes y vulnerabilidades de seguridad de la información.

5.8 PRUEBA DEL ESQUEMA DE ATENCIÓN DE INCIDENTES

La organización debería programar la verificación y las pruebas regulares de los procesos y procedimientos de gestión de incidentes de seguridad de la información, para destacar las fallas y los problemas potenciales que pueden surgir durante la gestión de eventos, incidentes y vulnerabilidades de la seguridad de la información. Se deberían organizar pruebas periódicas para verificar procesos/procedimientos y para verificar cómo responde el ISIRT a incidentes complejos severos, mediante el simulacro de ataques, fallas o defectos reales. Es conveniente prestar atención particular a la creación de escenarios simulados que deberían basarse en amenazas de seguridad de la información nuevas y reales. Las pruebas deberían involucrar no solamente al ISIRT, sino a todas las organizaciones internas y externas que están involucradas en la gestión de incidentes de seguridad de la información. Las organizaciones deberían asegurar que cualquier cambio hecho como resultado de revisiones posteriores a las pruebas se someta a una revisión profunda, incluso a pruebas adicionales, antes de que entre en funcionamiento el nuevo esquema.

6. FASE DE DETECCIÓN Y REPORTE

6.1 VISIÓN GENERAL SOBRE LAS ACTIVIDADES CLAVE

La primera fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información involucra la detección y recolección de información asociada con la ocurrencia de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de la información por medios humanos o automáticos, y el reporte de dichas ocurrencias. La gestión de incidentes de seguridad en funcionamiento comprende tres fases principales: fases de detección y reporte, evaluación y decisión (véase el numeral 7) y respuestas (véase el numeral 8). A continuación, está la fase de lecciones aprendidas (véase el numeral 9), en la que se identifican y hacen las mejoras. Estas fases y sus actividades asociadas se presentaron en el numeral 4.5.

Los siguientes numerales tratan principalmente sobre el manejo de eventos e incidentes de seguridad de la información. La organización debería asegurar que el personal adecuado trate las vulnerabilidades de seguridad de la información, de manera similar para conocer cómo se manejan las fallas de seguridad diferentes de la información, posiblemente con evaluación y resolución usando personal técnico (que pueden ser o no miembros del ISIRT). La información sobre vulnerabilidades y su resolución se debería ingresar a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información gestionados por el ISIRT. El Anexo D (informativo) presenta un ejemplo de plantilla de formato para reportar la vulnerabilidad en la seguridad de la información.

La Figura 3 presenta todas las fases operativas y actividades relacionadas.

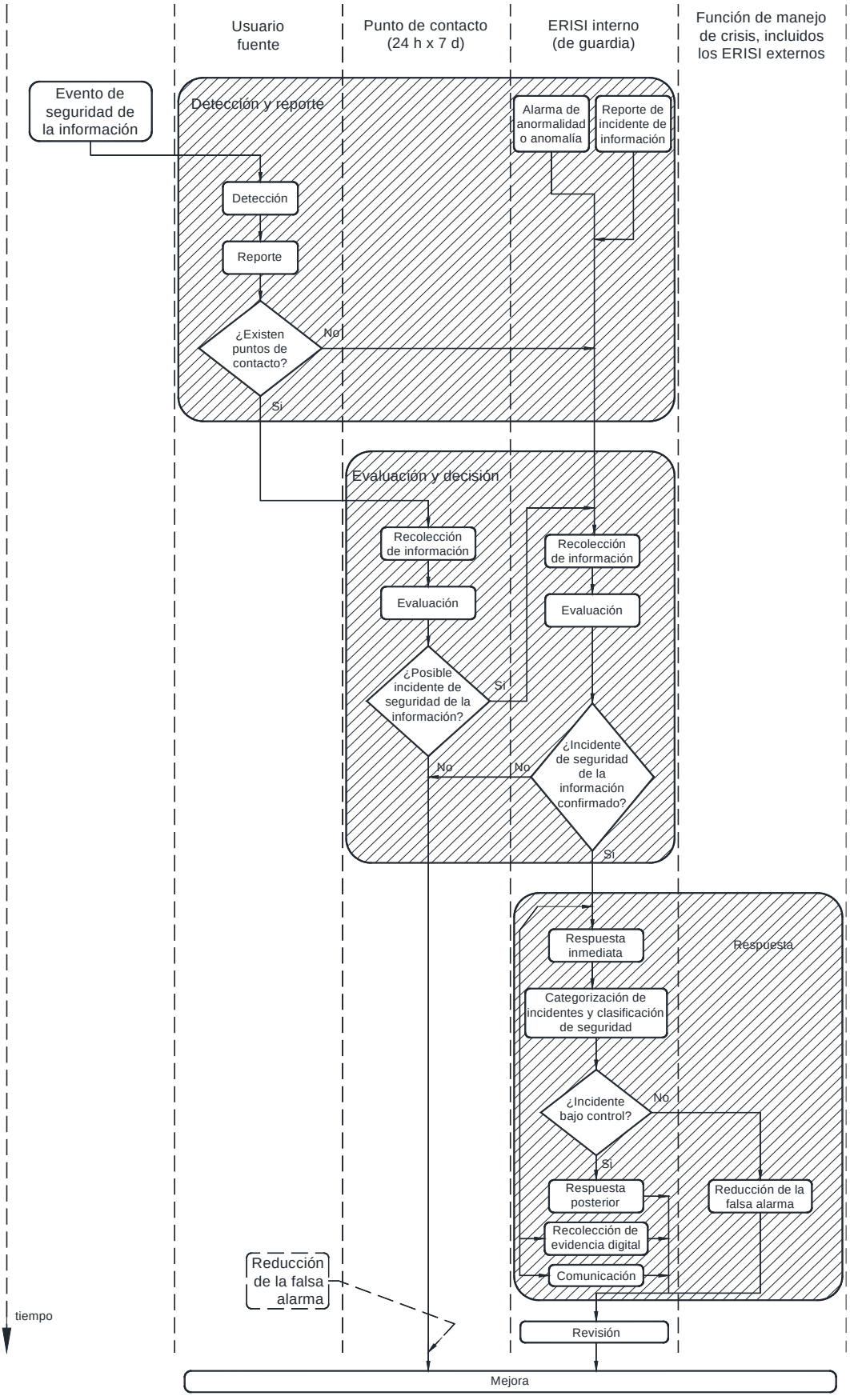

Figura 3. Diagrama de flujo de eventos e incidentes de seguridad de la información

NOTA Una falsa alarma es una identificación de un evento no deseado, pero se encuentra que no es real o no tiene consecuencias.

La primera fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información involucra la detección de las ocurrencias de eventos de seguridad de la información, la recolección de información asociada con ellas, y el reporte de dichas ocurrencias, por medios humanos o automáticos. La organización debería asegurar que esta fase involucre la detección de vulnerabilidades de seguridad de la información que aún no han sido aprovechadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, y reportarlos.

Para la fase de detección y reporte, una organización debería asegurar que las actividades clave sean las siguientes:

a) Actividad para detectar y reportar la ocurrencia de un evento de seguridad de la información, o la existencia de una vulnerabilidad de la seguridad de la información, ya sea por el personal o clientes de la organización, o automáticamente, con la ayuda de:

   1) alertas de sistemas de seguimiento de seguridad tales como IDS/IDP *(Intrusion Detection System / Intrusion Prevention System*) , programas antivirus, *honeypots* (término genérico para designar un sistema de señuelo usado para engañar, distraer, desviar y estimular al atacante hacia información que parece muy valiosa, pero que realmente es inventada y no sería de interés para un usuario legítimo [ISO/IEC 18043:2006[) / *Tarpits* (sistemas que están expuestos intencionalmente y diseñados para retardar ataques), sistemas de seguimiento de registros, sistemas de gestión de seguridad de la información, motores de correlación y otros,

   2) alertas de sistemas de seguimiento de redes, tales como cortafuegos, análisis de flujo de redes, filtrados de contenido y otros,

   3) análisis de información de registro de dispositivos, servicios, equipos y diversos sistemas,

   4) escalamiento de eventos anómalos detectados por el área de TIC,

   5) escalamiento de eventos anómalos detectados por las mesas de ayuda,

   6) reportes de usuarios, y

   7) notificaciones externas de terceras partes, tales como otros ISIRT, servicios de seguridad de la información, PSI, proveedores de servicios de telecomunicaciones, compañías de contratación externa o ISIRT nacionales.

b) Actividad para recolectar información sobre un evento o vulnerabilidad de seguridad de la información.

c) Actividad para asegurar que todos los involucrados en el PoC (Punto de Contacto) registren adecuadamente todas las actividades, resultados y decisiones relacionadas para análisis posterior.

d) Actividad para asegurar que se recolecta evidencia electrónica y se almacena en forma segura, y que se hace seguimiento continuo de su preservación segura, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas.

NOTA La futura Norma Internacional (ISO/IEC 27037) proporcionará información más detallada sobre la identificación, recolección, adquisición y preservación de evidencia digital.

e) Actividad para asegurar que el régimen de control de cambios se mantenga y cubra el seguimiento de los eventos y vulnerabilidades de seguridad de la información y las actualizaciones de reportes de eventos y vulnerabilidades, y de esta manera se mantenga actualizada la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

f) Actividad para escalar, según se requiera durante toda la fase, para revisión y/o decisiones posteriores.

g) Actividad para registrar en un Sistema de Seguimiento de Incidentes.

Toda la información recolectada correspondiente a un evento o vulnerabilidad de seguridad de la información se debería almacenar en la base de datos de eventos/incidentes/vulnerabilidades gestionada por el ISIRT. La información reportada durante cada actividad debería ser lo más completa posible en el momento, para asegurar que haya una buena base disponible para las evaluaciones y decisiones que se van a tomar, y por supuesto, las acciones que se van a tomar.

6.2 DETECCIÓN DE EVENTOS

Los eventos de seguridad de la información los puede(n) detectar directamente una(s) persona(s) que observe algo que le causa preocupación, ya sea relacionada con aspectos técnicos, físicos o procedimentales. La detección puede ser, por ejemplo, de detectores de fuego/humo, o alarmas para intrusos (ladrones) con alertas que notifican en lugares designados previamente para acción humana. Los eventos de seguridad técnica de la información se pueden detectar por medios automáticos, por ejemplo, alertas de instalaciones de análisis de rastreo de auditoría, cortafuegos, sistemas de detección de intrusión y herramientas contra códigos maliciosos (incluidos virus), en cada uno de los casos estimulados por parámetros preestablecidos.

Las posibles fuentes de detección de eventos de seguridad de la información incluyen las siguientes:

a) usuarios,

b) gerentes de línea y gerentes de seguridad,

c) clientes,

d) departamento de TI, incluido el Centro de Operaciones de Redes y el Centro de Operaciones de Seguridad (por medio de soporte en el segundo nivel),

e) mesa de ayuda de TI (por medio de soporte en el primer nivel),

f) proveedores de servicios gestionados (incluidos PSI, proveedores de servicios de telecomunicaciones, y proveedores),

g) ISIRT,

h) otras unidades y personal que pueden detectar anomalías durante su trabajo diario,

i) medios de comunicación (periódicos, televisión, etc.) y

j) sitios web (sitios web de información de seguridad pública, sitios web de investigadores de seguridad, sitios web de archivos corruptos, etc.).

6.3 REPORTE DE EVENTOS

Cualquiera que sea la fuente de detección de un evento de seguridad de la información, la persona notificada por un medio automático, o que observe directamente algo inusual, es responsable de iniciar el proceso de detección y reporte. Éste puede ser cualquier miembro del personal de una organización, ya sea contrato a término indefinido o fijo.

La persona debería seguir los procedimientos y usar el formato de reporte de eventos de seguridad de la información especificado en el esquema de gestión de incidentes de seguridad de la información, para llevar el evento de seguridad de la información al conocimiento del PoC (Punto de Contacto) y la gerencia. En consecuencia, es esencial que todo personal conozca bien y tenga acceso a las directrices para reportar los diferentes tipos de posibles eventos de seguridad de la información. Esto incluye el formato del formulario de reporte de eventos de seguridad de la información y detalles del personal al que se debería notificar en cada ocasión (todo el personal debería, al menos tener conocimiento del formato del formulario de reporte de incidentes de seguridad de la información, que les ayude a comprender el esquema.) Vale la pena mencionar que no se consideran seguros los teléfonos fijos, inalámbricos y celulares sin protección para interceptación. Cuando se maneja información muy confidencial o secreta, es conveniente colocar protecciones adicionales.

La siguiente información se puede usar como base para un formulario del sistema de rastreo de incidentes:

- hora/fecha de la detección,

- observaciones, e

- información de contacto (opcional).

El formulario completado (en papel, para envío por correo electrónico o mediante un formulario web) lo debería usar el personal de ISIRT, solamente cuando se registren incidentes de seguridad de la información en el Sistema de Rastreo de Incidentes. Es más significativo obtener conocimiento/reportes de un evento de seguridad de la información sospechado/experimentado/detectado que esté completo con toda la información.

El rastreo del evento de seguridad de la información (posiblemente incidente) se debería apoyar, siempre que sea posible, en una aplicación automatizada. El uso de un sistema de información es esencial para forzar al personal a seguir los procedimientos y listas de chequeo establecidos. También es extremadamente útil hacer el rastreo de “quién hizo qué, y cuándo lo hizo”, detalles que se pueden pasar por alto durante un evento de seguridad de la información (posiblemente incidente).

Cómo se maneje un evento de seguridad de la información dependerá de lo que se trate, y de las implicaciones y repercusiones que pueda tener. Para muchas personas, ésta será una decisión que se encuentra fuera de su competencia. Entonces, la persona que reporta un evento de seguridad de la información debería completar el formulario de reporte de eventos de seguridad de la información con su relato, lo más completo posible, y otra información que esté disponible en el momento, en enlace con su gerente local, si es necesario. Ese formulario se debería comunicar en forma segura al PoC (Punto de Contacto) designado, con una copia para el ISIRT responsable. De preferencia, el PoC (Punto de Contacto) debería suministrar un

servicio de 24 h durante siete días a la semana. El Anexo D (informativo) presenta un ejemplo de plantilla de formulario de reporte de eventos de seguridad de la información.

El ISIRT debería nombrar un miembro del equipo o delegado por turno de trabajo, que sea responsable de todos los reportes que llegan por correo electrónico, fax, formularios o conversaciones directas. Esta responsabilidad se puede rotar semanalmente entre los miembros del equipo. El miembro designado del equipo hace la evaluación y toma las acciones adecuadas para informar a las partes responsables y a las partes involucradas, y resolver el incidente de seguridad de la información.

Se hace énfasis en que no sólo es importante la exactitud, sino también la oportunidad del contenido incluido en el formulario de reporte de eventos de seguridad de la información. No es una buena práctica retrasar la presentación de un formulario de reporte para mejorar la exactitud de su contenido. Si la persona que reporta no está segura de los datos de alguno de los campos del formulario de reporte, se debería enviar con una anotación adecuada, y las actualizaciones se deberían comunicar posteriormente. También se debería reconocer que algunos mecanismos de reporte (por ejemplo, el correo electrónico) son en sí mismos objetivos visibles para el ataque.

Cuando existen problemas con los mecanismos de reporte electrónico (por ejemplo, correo electrónico), o se considera que existen, es conveniente usar medios de comunicación alternativos. Esto incluye también cuando se considere posible que el sistema esté bajo ataque y personas no autorizadas puedan leer los formularios de reporte electrónico. Los medios alternativos pueden ser: en persona, por teléfono o mensajes de texto. Estos medios alternativos se deberían usar cuando se hace particularmente evidente al inicio de una investigación, que un evento de seguridad de la información es posible que se clasifique como un incidente de seguridad de la información, particularmente uno que puede ser significativo.

Mientras que en muchos casos un evento de seguridad de la información debe ser reportado desde su inicio para que el PoC (Punto de Contacto) emprenda acciones, puede haber ocasiones en las que un evento de seguridad de la información de maneja localmente, posiblemente con ayuda de la gerencia local. Es recomendable que la gerencia local esté entrenada para hacer la misma evaluación que el ISIRT y para tomar las mismas contramedidas u otras similares, al igual que para usar el mismo sistema de rastreo de incidentes, de manera que localmente los recursos se utilicen con éxito. De esta manera se impedirá que el ISIRT lleve a cabo trabajo por duplicado.

Un evento de seguridad de la información se puede determinar rápidamente como una falsa alarma, o se puede resolver hasta que concluya satisfactoriamente. En estos casos, se debería llenar un formulario de reporte y enviarlo a la gerencia local, al PoC (Punto de Contacto) y al ISIRT. para propósitos de registro, es decir, a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información. En estas circunstancias, la persona que reporta un cierre de un evento de seguridad de la información está en capacidad de completar parcialmente la información requerida en el formulario de reporte de incidentes de seguridad de la información; si éste es el caso, entonces el formulario de reporte de incidentes de seguridad de la información también se debería completar y enviar. El uso de herramientas automáticas puede ayudar a completar algunos de los campos, por ejemplo, los sellos de registro de tiempo y también pueden ayudar a compartir/transferir la información necesaria.

7. FASE DE EVALUACIÓN Y DECISIÓN

7.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE

La segunda fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información involucra la evaluación de la información asociada con las ocurrencias de eventos de seguridad de la información, y la decisión acerca de si son incidentes de seguridad de la información.

Para la fase de evaluación y decisión, una organización debería asegurar que las actividades clave sean las siguientes:

a) Actividad para que el PoC (Punto de Contacto) evalúe y determine si un evento es un incidente de seguridad de la información posible o concluido, o es una falsa alarma, y si no es una falsa alarma, si se requiere escalarlo. Las evaluaciones deberían incluir el uso de la escala acordada de clasificación de eventos/incidentes de seguridad de la información (incluida la determinación del impacto de los eventos con base en los activos/servicios afectados) y decidir si los eventos se deberían clasificar como incidentes de seguridad de la información (véanse ejemplos de orientación en el Anexo C). Mientras se determinan los impactos de los eventos de seguridad de la información (y los posibles incidentes) en términos de los efectos de violación de la confidencialidad, integridad y disponibilidad, las organizaciones deberían asegurar que se identifique lo siguiente:

   1) dominio del impacto (físico o lógico),

   2) activos, infraestructuras, información, procesos, servicios y aplicaciones afectadas o que se van a ver afectados, y

   3) los posibles efectos en los servicios esenciales de la organización.

b) Actividad para que el ISIRT lleve a cabo la evaluación para confirmar los resultados de la evaluación del PoC (Punto de Contacto), ya sea que el evento sea o no un incidente de seguridad de la información, si es aplicable. Si es necesario, se debería llevar a cabo otra evaluación usando la escala acordada de clasificación de eventos/incidentes de seguridad de la información, con detalles del tipo de evento (posiblemente incidente) y recurso afectado (categorización) (véase un ejemplo de directrices en el Anexo C (informativo)). A continuación se deberían tomar las decisiones acerca de cómo se debería tratar el incidente de seguridad confirmado, por quién y con qué prioridad. Esto debería involucrar el proceso de priorización predeterminado para posibilitar un enfoque claro para la asignación de cada incidente de seguridad de la información a las personas adecuadas, y determinar la urgencia del manejo y las respuestas al incidente de seguridad de la información que incluyan, ya sea una respuesta inmediata, el análisis forense de seguridad de la información y las actividades de comunicación requeridas, en la fase siguiente (Respuestas, véase también el numeral 8).

c) Actividad para escalar, según se requiera durante toda la fase, para evaluaciones y/o decisiones posteriores.

d) Actividad para asegurar que todos los involucrados, particularmente el ISIRT, registran adecuadamente todas las actividades para análisis posterior.

e) Actividad para asegurar que se recolecta evidencia electrónica y se almacena en forma segura, y que se hace seguimiento continuo de su preservación segura, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas.

f) Actividad para asegurar que el régimen de control de cambios se mantenga y cubra el rastreo de incidentes de seguridad de la información y las actualizaciones de reportes de incidentes de seguridad de la información, y de esta manera, se mantenga actualizada la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Toda la información recolectada correspondiente a un evento/incidente/vulnerabilidad de la información se debería almacenar en una base de datos de eventos/incidentes/vulnerabilidades gestionada por el ISIRT. La información reportada durante cada actividad debería ser lo más completa posible en el momento, para asegurar que haya una buena base disponible para las evaluaciones y decisiones que se van a tomar, y para las acciones que se van a tomar.

Una vez que el evento de seguridad haya sido detectado y reportado, se llevan a cabo las siguientes actividades:

g) Actividad para distribuir la responsabilidad por las actividades de gestión de incidentes de seguridad de la información, a través de la jerarquía de personal adecuada, en donde las acciones de evaluación, toma de decisiones y acciones involucran personal de seguridad y personal diferente de éste.

h) Actividad para suministrar procedimientos formales que debe seguir cada persona notificada, incluida la revisión y corrección del reporte, la evaluación de daños y la notificación al personal pertinente (las acciones individuales dependen del tipo y severidad del incidente).

i) Actividad para usar directrices para una documentación minuciosa de un evento de seguridad de la información.

j) Actividad de uso de directrices para una documentación minuciosa de las acciones posteriores a un incidente de seguridad de la información, si el evento de seguridad de la información se llega a clasificar como un incidente de seguridad de la información.

k) Actividad de actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

La organización debería asegurar que esta fase involucra la evaluación de la información recolectada en las vulnerabilidades de la seguridad de la información reportadas (que aún no han sido aprovechadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información), y las decisiones acerca de cuál necesita tratarse, quién la va a tratar y con qué prioridad.

7.2 EVALUACIÓN Y DECISIÓN INICIAL POR EL PoC (PUNTO DE CONTACTO)

La persona en el PoC (Punto de Contacto) que recibe el formulario de reporte de eventos de seguridad de la información debería acusar recibo de éste, ingresarlo en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, y revisarlo. Debería buscar cualquier aclaración de parte de la persona que reporta el evento de seguridad de la información, y recoger la información adicional que se requiera y que se tenga conocimiento de que está disponible, ya sea de parte de la persona que hace el reporte o de alguna otra. Luego

el PoC debería llevar a cabo una evaluación para determinar si el evento de seguridad de la información se debería clasificar como un incidente de seguridad de la información o de si el hecho es una falsa alarma (incluido el uso riguroso de una escala acordada de clasificación de incidentes, de la organización). Si se determina que el evento de seguridad de la información es una falsa alarma, el formulario de reporte de eventos de seguridad de la información se debería completar y comunicar al ISIRT para adicionarlo a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información y revisarlo, y enviar copia a la persona que hizo el reporte y a su gerente local.

La información y otra evidencia recolectada en esta etapa pueden ser necesarias en el futuro para acciones disciplinarias o legales. La(s) persona(s) que realiza(n) las tareas de recolección y evaluación de información debería(n) recibir formación en los requisitos para recolección y preservación de evidencia.

Además de registrar la(s) fecha(s) y hora(s) de las acciones, es necesario documentar completamente lo siguiente:

a) qué se observó y qué se hizo (incluyendo las herramientas usadas) y por qué;

b) la ubicación de la evidencia potencial;

c) cómo se archivó la evidencia (si es aplicable),

d) cómo se llevó a cabo la verificación de la evidencia (si es aplicable), y

e) detalles del almacenamiento/custodia segura del material y del acceso posterior a él.

Si se determina que el evento de seguridad de la información es un probable incidente de seguridad de la información, y si la persona del PoC (Punto de Contacto) tiene el nivel de competencia adecuado, se puede llevar a cabo una evaluación posterior. Esto puede requerir acciones remediales, por ejemplo, la identificación de controles de emergencia adicionales y su remisión a la persona adecuada, para la toma de acciones. Puede ser evidente que un evento de seguridad se determina como un incidente significativo de seguridad de la información (usando la escala de severidad predeterminada de la organización), en cuyo caso se debería informar directamente al líder del ISIRT. Puede ser evidente que se debería declarar una situación de crisis, y por ejemplo, el líder de gestión de crisis se debería notificar para la activación posible de un plan de manejo de crisis, y se debería informar al líder del ISIRT y a la alta dirección. Sin embargo, la situación más probable es que el incidente de seguridad de la información deba remitirse directamente al ISIRT para evaluación y acción posterior.

Cualquiera que sea el paso siguiente que se determine, el PoC (Punto de Contacto) debería completar lo más posible el formulario de reporte de incidentes de seguridad de la información. El formulario de reporte de incidentes de seguridad de la información debería incluir el relato de lo sucedido, y en la medida de lo posible, debería confirmar y describir lo siguiente:

a) en qué consiste el incidente de seguridad de la información;

b) cómo fue causado, y qué o quién lo causó;

c) a qué afecta o podría afectar;

d) el impacto real o potencial del incidente de seguridad de la información en el negocio de la organización;

e) una indicación en cuanto si el incidente de seguridad de la información se considera significativo o no (usando la escala de clasificación predeterminada de la organización), y

f) cómo se ha tratado hasta el momento.

Cuando se consideran los efectos adversos reales o potenciales de un incidente de seguridad de la información en el negocio de una organización, los siguientes son algunos ejemplos de ellos:

a) divulgación no autorizada de información;

b) modificación no autorizada de información;

c) repudio de información;

d) no disponibilidad de información y/o servicio;

e) destrucción de de información y/o servicio;

f) desempeño reducido del servicio.

El primer paso es considerar cuál, de entre varias consecuencias, es pertinente. Para las que se consideran pertinentes, se debería usar la directriz de la categoría relacionada, para establecer los impactos reales y potenciales y registrarlos en el reporte de incidentes de seguridad de la información. En el Anexo C (Informativo) se presentan ejemplos de directrices. Algunos ejemplos de estas categorías son:

a) pérdida financiera/interrupción en las operaciones del negocio;

b) intereses comerciales y económicos;

c) información personal;

d) obligaciones legales y reglamentarias;

e) operaciones de gestión y del negocio;

f) pérdida del buen nombre;

g) lesiones o fallecimiento, y

h) perturbación para la sociedad.

Si se ha solucionado un incidente de seguridad de la información, el reporte debería incluir los detalles de los controles que se han llevado a cabo y las lecciones aprendidas (por ejemplo, los controles que se van a adoptar para impedir nuevas ocurrencias u ocurrencias similares). Una vez que el formulario de reporte se haya completado lo más posible, entonces se debería enviar al ISIRT para su registro en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información y para su revisión.

Si es posible que una investigación tome un período más largo que el definido en la política de gestión de incidentes de seguridad de la información, es conveniente elaborar un informe temporal dentro del período de tiempo especificado en la política.

Se hace énfasis en que el PoC (Punto de Contacto) que evalúa un incidente de seguridad de la información debería tener conocimiento de los siguientes aspectos, con base en las directrices suministradas en la documentación del esquema de gestión de incidentes de seguridad de la información. Por ejemplo, incluye lo siguiente:

a) cuándo es necesario escalar el asunto, y a quién llevarlo;

b) los procedimientos de control de cambios se deberían seguir en todas las actividades realizadas por el PoC (Punto de Contacto), y

c) de manera similar a lo mencionado en los numerales 6.2 y 6.3 anteriores, en relación con la detección y reporte de eventos, se deberían usar medios de comunicación alternativos para los formularios de reporte actualizados, cuando existan o se considera que existen problemas con los mecanismos de reporte electrónico (por ejemplo, correo electrónico).

7.3 EVALUACIÓN Y CONFIRMACIÓN DEL INCIDENTE POR EL ISIRT

La evaluación y confirmación de la decisión en cuanto a si el evento de seguridad de la información se va clasificar como un incidente de seguridad de la información debería ser responsabilidad del ISIRT. La persona que recibe el reporte en el ISIRT debería hacer lo siguiente:

a) acusar recibo del formulario de reporte del incidente de seguridad de la información completado de la manera más exhaustiva posible por el PC;

b) ingresar el formato a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información si esto no lo ha hecho el PC, y actualizar la base de datos si es necesario;

c) buscar aclaración del PC, si es necesario;

d) revisar el contenido del formulario de reporte, y

e) recolectar cualquier información adicional que se requiera y que se tenga conocimiento de que está disponible, ya sea de parte del PC, de la persona que completó el formulario de reporte del evento de seguridad de la información o de alguna otra.

Si continúa habiendo algún grado de incertidumbre en cuanto a la autenticidad del incidente de seguridad de la información o a que la información reportada esté completa, el miembro de ISIRT debería llevar a cabo una evaluación para determinar si el incidente de seguridad de la información es real, o es una falsa alarma (mediante el uso de la escala de clasificación de incidentes acordada por la organización). Si se determina que el incidente de seguridad es una falsa alarma, el formulario de reporte de eventos de seguridad de la información se debería completar, adicionar a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, y comunicar al líder del ISIRT. Se deberían enviar copias del reporte al PC, a la persona que hizo el reporte y a su gerente local.

Un incidente de seguridad de la información se debería correlacionar con cualquier otro evento/incidente reportado al ISIRT. Esta importante actividad tiene como fin verificar si el incidente está relacionado con cualquier otro evento/incidente, o si es simplemente el efecto de otro incidente, es decir, ataque de denegación de servicio (sigla en inglés DoS) y ataques de denegación de servicio distribuidos (sigla en inglés DoS). La correlación de incidentes también es importante al priorizar los esfuerzos del ISIRT.

Si se determina que el incidente de seguridad de la información es real, el miembro del ISIRT y sus colegas, según se requiera, deberían llevar a cabo la evaluación posterior. El objetivo es confirmar lo más pronto posible:

a) En qué consiste el incidente de seguridad de la información, cómo se originó o quién lo originó, qué afecta o puede afectar, su impacto real o potencial en los negocios de la organización, una indicación en cuanto a si el incidente de seguridad de la información se considera significativo o no (usando la escala predeterminada de severidad de la organización). Si el incidente causa impacto negativo severo en el negocio, se deberían iniciar actividades de crisis (véase el numeral 8.2.4).

b) Los siguientes aspectos acerca de ataque técnico deliberado por una persona sobre un sistema, servicio y/o red de información, por ejemplo:

   1) en qué grado el sistema, servicio y/o red ha sido infiltrado, y qué nivel de control tiene el atacante,

   2) a qué datos ha ingresado el atacante, posiblemente ha copiado, alterado o destruido, y

   3) qué software ha sido copiado, alterado o destruido por el atacante.

c) Los efectos directos e indirectos (por ejemplo, el acceso físico queda abierto debido a un incendio, el sistema de información es vulnerable debido a un mal funcionamiento del software o de la línea de comunicaciones, o debido a error humano).

d) Cómo se ha tratado hasta la fecha el incidente de seguridad de la información, y por quién.

Cuando se examinan los efectos adversos reales o potenciales de un incidente de seguridad de la información en el negocio de una organización, de alguna información y/o servicios que se presentan en el numeral 7.2, es necesario confirmar cuál de las consecuencias es pertinente. En el numeral 7.2 y en el Anexo C se presentan ejemplos de categorías.

Es conveniente usar un proceso de priorización para asignar un incidente de seguridad de la información a la persona o grupo de personas más adecuadas en el ISIRT, para facilitar una respuesta adecuada al incidente de seguridad de la información. En particular, cuando se están tratando a la vez varios incidentes de seguridad de la información, es necesario establecer prioridades para ordenar las respuestas que se van a dar a los incidentes de seguridad de la información.

Las prioridades se deberían establecer, de acuerdo con los impactos adversos para el negocio asociados con el incidente de seguridad de la información y el esfuerzo estimado necesario para responder a dicho incidente. Para incidentes con la misma prioridad, el esfuerzo requerido es una métrica para determinar el orden en el que es necesario responder. Por ejemplo, un incidente de fácil resolución se puede tratar antes de un incidente que requiere un esfuerzo mayor.

Para los que se consideran pertinentes, se debería usar la directriz de la categoría relacionada, para establecer los impactos reales y potenciales y registrarlos en el reporte de incidentes de seguridad de la información. En los Anexos C y D se presentan ejemplos de directrices.

8. FASE DE RESPUESTAS

8.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE

La tercera fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información involucra dar respuesta a incidentes de seguridad de la información, según las acciones acordadas en la fase de evaluación y decisión. Dependiendo de las decisiones, las respuestas se pueden ejecutar de inmediato, en tiempo real o casi real, y algunas pueden involucrar el análisis forense de seguridad de la información.

Para la fase de respuestas, una organización debería asegurar que las actividades clave sean las siguientes:

a) Actividad de revisión, por parte del ISIRT, para determinar si el incidente de seguridad de la información está bajo control, y la actividad siguiente:

   1) Actividad para promover la respuesta requerida, si está bajo control. Ésta puede ser una respuesta inmediata que puede incluir la activación de los procedimientos de recuperación, o la expedición de comunicaciones al personal involucrado pertinente, o una respuesta posterior más lenta (por ejemplo, al facilitar la recuperación lenta de un desastre), mientras se asegura que toda la información esté lista para actividades de revisión posteriores al incidente.

   2) Actividad para promover actividades de crisis al llevar el incidente a la función de manejo de crisis, si no está bajo control o si va a tener un impacto severo en los servicios esenciales de la organización (véase también el numeral 8.2.4). La función de manejo de crisis es entonces responsable del incidente, con el soporte total del ISIRT (incluyendo entre otras, la activación de un plan de gestión de crisis), e involucrando al personal relacionado, por ejemplo, el líder y el equipo de gestión de crisis de la organización (para orientación sobre gestión de la continuidad del negocio, véase la ISO/IEC 27031 e ISO/PAS 22399:2007).

b) Actividad para asignar recursos internos e identificar recursos externos para responder a un incidente.

c) Actividad para llevar a cabo el análisis forense de seguridad de la información, según se requiera, y en relación con la calificación de la escala de clasificación de incidentes de seguridad de la información, y al cambio de la calificación en la escala, si es necesario.

d) Actividad para escalar el incidente, según se requiera, durante toda la fase, para revisiones o decisiones posteriores.

e) Actividad para asegurar que todos los involucrados, particularmente el ISIRT, registran adecuadamente todas las actividades para análisis posterior.

f) Actividad para asegurar que se recolecta evidencia electrónica y se almacena en forma segura, de manera comprobable, y que se hace seguimiento continuo de su preservación segura, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas.

g) Actividad para asegurar que el régimen de control de cambios se mantenga y cubra el rastreo de incidentes de seguridad de la información y las actualizaciones de reportes de incidentes de seguridad de la información, y de esta manera se mantenga

actualizada la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

h) Actividad para comunicar la existencia del incidente de seguridad de la información o cualquier detalle pertinente de éste a otras organizaciones o personas internas o externas, en particular a los dueños de activos/información/servicios particulares (determinados durante el análisis de impacto) y a organizaciones internas/externas que deberían estar involucradas en la gestión y resolución del incidente.

Toda la información recolectada correspondiente a un evento, incidente o vulnerabilidad de seguridad de la información se debería almacenar en una base de datos de eventos/incidentes/vulnerabilidades gestionada por el ISIRT, incluida con propósitos de análisis posteriores. La información reportada durante cada actividad debería ser lo más completa posible en el momento, para asegurar que haya una buena base disponible para las evaluaciones y decisiones que se van a tomar, y por supuesto, de las acciones tomadas.

Una vez que se haya determinado el incidente de seguridad de la información y se hayan acordado las respuestas, las actividades posteriores son las siguientes:

a) Actividad para distribuir la responsabilidad de las actividades de gestión de incidentes a través de la jerarquía de personal adecuada, en donde la toma de decisiones y las acciones involucra personal de seguridad y personal diferente de éste.

b) Actividad de suministro de procedimientos formales que debe seguir cada persona involucrada, incluida la revisión y corrección de reportes, la reevaluación de daños y la notificación al personal pertinente (las acciones individuales dependen del tipo y severidad del incidente).

c) Actividad de uso de directrices para una documentación minuciosa de un incidente de seguridad de la información, de las acciones posteriores y de la actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

d) Actividad de uso de directrices para una documentación minuciosa de las acciones posteriores.

e) Actividad de actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Una vez que el incidente de seguridad de la información se haya tratado exitosamente, se debería cerrar formalmente y esto se debería registrar en la base de datos de gestión de incidentes de seguridad de la información. La organización también debería asegurar que esta fase involucre también dar respuesta a las vulnerabilidades de seguridad de la información reportadas, según las acciones acordadas en la fase de evaluación y decisión. Una vez que la vulnerabilidad se haya tratado, los detalles se deberían registrar en la base de datos de gestión de incidentes de seguridad de la información.

En el numeral 8.2 se presentan directrices sobre las respuestas a incidentes de seguridad de la información.

8.2 RESPUESTAS

8.2.1 Respuestas inmediatas

8.2.1.1 Visión general

En la mayoría de casos, las actividades siguientes que debe llevar a cabo el miembro del ISIRT son: identificar las acciones de respuesta inmediata para tratar el incidente de seguridad de la información, registrar los detalles en el formulario de incidentes de seguridad de la información y dentro de la base de datos de eventos/incidentes/vulnerabilidades, y notificar las acciones requeridas a las personas o grupos adecuados. Esto puede dar como resultado controles de emergencia (por ejemplo, interrupción o clausura de un sistema, servicio y/o red afectado, con aceptación previa de la gerencia de TI y/o del negocio pertinente), y/o identificación de controles permanentes adicionales, y notificación de acciones a la persona o grupo adecuado de ISO/IEC. Si no se ha determinado aún la importancia del incidente de seguridad de la información, esto se debería hacer usando la escala de clasificación predeterminada de la organización, y si es lo suficientemente significativa, se debería notificar directamente a la alta gerencia adecuada. Si es evidente que se debería declarar una situación de crisis, por ejemplo, se debería notificar al líder de gestión de crisis para la activación posible de un plan de manejo de crisis, y se debería informar al líder del ISIRT y a la alta dirección.

Los objetivos generales para responder a los incidentes de seguridad de la información son los siguientes:

a) confinar los impactos potenciales adversos (de los incidentes de seguridad de la información), y

b) mejorar la seguridad de la información.

La meta primaria del esquema de gestión de incidentes de seguridad de la información y de las actividades asociadas debería ser la minimización de los impactos adversos para el negocio, mientras que la identificación del atacante se debería considerar una meta secundaria.

8.2.1.2 Ejemplo de acciones

Un ejemplo de acciones de respuesta pertinentes inmediatas, en el caso de ataque deliberado a un sistema, servicio o red de información, o ambos, es que éste se puede dejar conectado a la Internet o a otra red. Esto permitirá que las aplicaciones críticas del negocio funcionen correctamente y recolecten tanta información como sea posible acerca del atacante, siempre que éste no sepa que está bajo vigilancia.

Es de vital importancia seguir los procesos planificados y registrar las acciones. Se debe tener cuidado con los troyanos, *rootkits* y módulos *kernel*, que pueden causar un daño grave al sistema. La evidencia se puede proteger mediante criptografía, seguros y registros de acceso.

a) Mientras se toma esta decisión, es necesario considerar que el atacante se puede dar cuenta de que es observado y pueda tomar acciones que causen más daño al sistema, servicio y/o red de información afectado y a los datos relacionados, y puede destruir la información que puede ser útil para rastrearlo.

b) Es esencial que sea técnicamente posible interrumpir o apagar rápidamente y en forma confiable el sistema, servicio y/o red de información atacada, una vez que se haya tomado una decisión. Esto sirve para contener el incidente.

Una consideración adicional es que la prevención de una nueva ocurrencia usualmente tiene una alta prioridad, y se podría concluir que el atacante ha expuesto una vulnerabilidad que se debería rectificar, y que los beneficios obtenidos de rastrearlo no justifican el esfuerzo de hacerlo. Esto es especialmente pertinente cuando el atacante no es malicioso y ha causado poco o ningún daño.

En relación con los incidentes de seguridad de la información que no son causados por un ataque deliberado, la fuente se debería identificar. Puede ser necesario apagar el sistema, servicio o red de información, o aislar la parte pertinente y apagarla (con la aceptación previa de la gerencia de IT y/o de gestión del sistema pertinente) mientras se implementan los controles. Esto puede tomar más tiempo si la vulnerabilidad es fundamental para el diseño del sistema, servicio y/o red, o si es crítica.

Otra actividad de respuesta puede ser activar técnicas de vigilancia (por ejemplo, *honeypots,* véase la ISO/IEC 18043). Esto se debería hacer con base en procedimientos documentados para el esquema de gestión de incidentes de seguridad de la información.

El miembro de ISIRT debería verificar la información que se puede corromper por un incidente de seguridad de la información, contra los registros de respaldo, para determinar modificaciones, eliminaciones o inserciones de información. Puede ser necesario verificar la integridad de los registros, ya que un atacante deliberado puede haber manipulado estos registros para cubrir su rastro.

8.2.1.3 Actualización de la información de incidentes

Cualquiera que sea el paso siguiente, el miembro de ISIRT debería actualizar el reporte del incidente de seguridad de la información tanto como sea posible, agregarlo a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, y notificar al líder del ISIRT y a otros, según sea necesario. Además, la actualización puede comprender información sobre lo siguiente:

a) en qué consiste el incidente de seguridad de la información,

b) cómo fue causado, y qué o quién lo causó,

c) qué afecta o podría afectar,

d) el impacto real o potencial del incidente de seguridad de la información en el negocio de la organización,

e) cambios en la indicación de si el incidente de seguridad de la información se considera significativo o no (usando la escala predeterminada de clasificación de severidad de la organización), y

f) cómo se ha tratado hasta el momento.

Si se ha solucionado un incidente de seguridad de la información, el reporte debería incluir los detalles de los controles que se han llevado a cabo y las lecciones aprendidas (por ejemplo, los controles que se van a adoptar para impedir nuevas ocurrencias u ocurrencias similares). El reporte actualizado se debería agregar a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, y se debería notificar al líder del ISIRT y a otros, según se requiera.

Se hace énfasis en que el ISIRT es responsable de asegurar la retención de toda la información pertinente al incidente de seguridad de la información para análisis posterior, y uso potencial legal como evidencia. Por ejemplo, para un incidente de seguridad de la información orientado a TI, se deberían emprender las siguientes acciones.

Después del descubrimiento inicial del incidente, todos los datos volátiles se deberían recolectar antes de apagar el sistema, servicio y/o red de TI afectada, para una investigación forense completa de seguridad de la información. La información por recolectar incluye los contenidos de memoria, cache y registros, y detalle de cualquier actividad que se esté realizando, y lo siguiente:

a) Se debería elaborar un duplicado forense completo de seguridad de la información del sistema afectado, o un archivo de respaldo de bajo nivel de registros y archivos importantes, dependiendo de la naturaleza del incidente de seguridad de la información.

b) Se deberían recolectar y revisar los registros de los sistemas, servicios y redes vecinas, por ejemplo, incluidos los de los enrutadores y cortafuegos.

c) Toda la información recolectada se debería almacenar en forma segura en modo de lectura solamente.

d) Mientras se lleva a cabo la duplicación forense de seguridad de la información es conveniente que haya al menos dos personas que afirmen y certifiquen que todas las actividades se han llevado a cabo, de acuerdo con la legislación y la reglamentación pertinente.

e) Las especificaciones y descripciones de las herramientas y comandos usados para llevar a cabo la duplicación forense de seguridad de la información se deberían documentar y almacenar junto con los medios originales.

Un miembro de ISIRT también es responsable de facilitar el regreso de la función afectada (ya sea de TI u otra) a un estado operativo seguro que no sea susceptible de estar en peligro nuevamente por el mismo ataque, si es posible en esta etapa.

8.2.1.4 Actividades adicionales

Si un miembro de ISIRT determina que un incidente de seguridad de la información es real, entonces se deberían llevar a cabo otras actividades importantes:

a) actividad para dar inicio al análisis forense de seguridad de la información, y

b) actividad para informar a los responsables de las comunicaciones internas y externas acerca de los hechos y propuestas que se deberían comunicar, en qué forma y a quién.

Una vez que un reporte del incidente de seguridad de la información se haya completado en la medida de lo posible, se debería ingresar en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, y comunicar al líder del ISIRT.

Si es probable que una investigación tome un tiempo mayor al acordado previamente dentro de la organización, se debería producir un reporte temporal.

El miembro del ISIRT que evalúa un incidente de seguridad de la información debería tener conocimiento de lo siguiente, entre otros, con base en las directrices suministradas en la documentación del esquema de gestión de incidentes de seguridad de la información:

a) cuándo es necesario escalar los asuntos, y a quién llevarlos, y

b) los procedimientos de control de cambios se deberían seguir en todas las actividades realizadas por el ISIRT.

Cuando existen problemas, o se considera que existen, con las funciones de comunicaciones electrónicas (por ejemplo, correo electrónico o web), incluyendo cuando es posible que el sistema sea atacado, el reporte a las personas pertinentes se debería hacer por teléfono o mensaje de texto.

Si se concluye que un incidente de seguridad de la información es significativo, o se ha determinado que hay una situación de crisis, el líder del ISIRT, en coordinación con el líder de seguridad de la información y los representantes pertinentes de la alta dirección/miembros, deberían ponerse en contacto con las partes relacionadas, tanto internas como externas a la organización.

Para asegurar que estos enlaces se organicen rápidamente y en forma eficaz, es necesario establecer de antemano un método de comunicación seguro que no dependa completamente del sistema, servicio y/o red que se puede ver afectado por el incidente de seguridad de la información. Estas medidas pueden incluir la designación de asesores o representantes de respaldo, en caso de ausencia.

8.2.2 Evaluación del control de incidentes de seguridad de la información

Después de que el miembro del ISIRT haya promovido respuestas inmediatas y actividades de comunicaciones y análisis forenses de seguridad de la información, es necesario determinar rápidamente si el incidente de seguridad de la información está bajo control. Si es necesario, el miembro de ISIRT puede consultar a sus colegas, al líder de ISIRT y a otras personas o grupos.

Si se confirma que el incidente de seguridad de la información está bajo control, el miembro del ISIRT debería dar inicio a:

Cualquier respuesta posterior requerida al análisis forense de seguridad de la información, y las comunicaciones pertinentes para dar fin al incidente de seguridad de la información y restaurar el sistema de información afectado para que las operaciones regresen a la normalidad.

Si se confirma que el incidente de seguridad de la información no está bajo control, el miembro de ISIRT debería dar inicio a actividades de crisis.

Si el incidente de seguridad de la información está relacionado con pérdida de disponibilidad, la métrica para evaluar si un incidente de seguridad de la información está bajo control, puede ser el tiempo transcurrido antes de regresar a una situación normal, después de la ocurrencia de un incidente de seguridad de la información. La organización debería determinar para cada activo, con base en los resultados de la evaluación de riesgos de seguridad de la información, su ventana de interrupción aceptable que apoye el tiempo objetivo de recuperación antes de que se reanude el servicio o el acceso a la información. Tan pronto la respuesta exceda la ventana de interrupción aceptable del activo objetivo, el incidente de seguridad de la información puede no estar más bajo control, y se debería tomar la decisión de escalar este incidente. Los incidentes de seguridad de la información relacionados con la pérdida de

confidencialidad, integridad, etc., necesitan otro tipo de criterios para determinar si la situación está bajo control y las posibles métricas de acuerdo con los planes de gestión de crisis de la organización.

8.2.3 Respuestas posteriores

Una vez que se ha determinado que un incidente de seguridad de la información está bajo control, y no sujeto a las actividades de crisis, el miembro del ISIRT debería identificar si se requieren respuestas adicionales para tratar el incidente de seguridad de la información. Esto puede incluir la restauración del sistema(s), servicio(s) y/o red(es) de información a su operación normal. Entonces se deberían registrar los detalles en el formulario de reporte de incidentes de seguridad de la información y en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información y notificar a los responsables de llevar a cabo las acciones relacionadas. Una vez que estas acciones se hayan llevado a cabo con éxito, los detalles se deberían registrar en el formulario de reporte de incidentes de seguridad de la información y en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información y luego el incidente de seguridad de la información debería ser cerrado y notificado al personal pertinente.

Algunas respuestas están dirigidas a impedir que ocurra nuevamente el incidente de seguridad de la información, u otra ocurrencia similar. Por ejemplo, si se determina que la causa de un incidente de seguridad de la información es una falla en el hardware o software de TI, debido a la ausencia de un parche, se debería contactar de inmediato al proveedor. Si una vulnerabilidad de TI conocida estuvo involucrada en un incidente de seguridad de la información, se debería corregir con la actualización de seguridad de la información pertinente. A partir de entonces se debería tratar cualquier problema relacionado con configuración de TI que haya puesto en evidencia el incidente de seguridad de la información. Otras medidas para reducir la posibilidad de que ocurra nuevamente el mismo incidente de seguridad de la información de TI o uno similar, pueden incluir el cambio de contraseñas del sistema y la deshabilitación de servicios no utilizados.

Otra área de actividad de respuesta puede involucrar hacer seguimiento del sistema, servicio y/o red de TI. Posterior a la evaluación de un incidente de seguridad de la información, puede ser adecuado implementar controles de seguimiento adicionales para ayudar a detectar eventos inusuales o sospechosos que serían sintomáticos de otros incidentes de seguridad de la información. Este seguimiento también puede revelar mayor profundidad del incidente de seguridad de la información e identificar otros sistemas de TI que estuvieran en riesgo.

También puede ser muy necesario para la activación de respuestas específicas documentadas en el plan pertinente de gestión de crisis. Esto se puede aplicar a incidentes de seguridad de la información relacionados o no con TI. Estas respuestas deberían incluir las relacionadas con aspectos del negocio, no solo directamente relacionadas con TI sino los relacionados con mantenimiento de funciones clave del negocio y posterior restauración, incluidas, si son pertinentes, aplicaciones de telecomunicaciones de voz, aplicaciones a niveles personales e instalaciones físicas.

La última área de actividad es la restauración de sistema(s), servicio(s) y/o red(es) de información afectados a operación normal. La restauración de un(os) sistema(s), servicio(s) y/o red(es) a un estado operativo seguro se puede lograr mediante la aplicación de parches a vulnerabilidades conocidas, o mediante la deshabilitación de algún elemento que estaba en peligro. Si se desconoce el alcance completo del incidente de seguridad de la información, debido a la destrucción de registros durante el incidente, entonces puede ser necesario reconstruir el sistema, servicio o red completos. También puede ser muy necesario para la activación de partes del plan pertinente de gestión de crisis.

Si un incidente de seguridad de la información no está relacionado con TI, por ejemplo, es causado por un incendio, una inundación o una bomba, entonces las actividades de recuperación que se deben seguir son las que están documentadas en el plan de gestión de crisis.

8.2.4 Respuestas a situaciones de crisis

Como ya se discutió en el numeral 8.2.2, es posible que el ISIRT determine que un incidente de seguridad de la información no está bajo control y necesita llevarlo al nivel de situación de crisis, usando un plan prediseñado.

Las mejores opciones para tratar todos los tipos posibles de incidentes de seguridad de la información que podrían afectar la disponibilidad y en alguna medida la integridad de un sistema de información, se deberían haber identificado en el plan de gestión de crisis de la organización. Estas opciones deberían estar directamente relacionadas con las prioridades de los negocios de la organización y con las escalas de tiempo relacionadas para la recuperación, y en consecuencia, con los períodos de tiempo de interrupción máximos aceptables para TI, voz, personas y alojamiento. La estrategia debería haber identificado lo siguiente:

a) las medidas requeridas de gestión de crisis, resiliencia y preventivas;

b) la estructura y responsabilidades organizacionales requeridas para responder a la crisis, y la estructura y el contenido requerido para el(los) plan(es) de gestión de crisis.

El(los) plan(es) de gestión de crisis y los controles implementados para apoyar la activación de estos planes, una vez que se han puesto a prueba satisfactoriamente, forman la base para abordar la mayoría de incidentes que se han escalado, una vez que se han designado como tales.

Dependiendo del tipo de incidente, y si no se encuentra bajo control, el escalarlo puede conducir a actividades cruciales para tratar el incidente, y activar el plan de gestión de crisis, si está implementado. Estas actividades pueden incluir, entre otras, la activación de:

a) instalaciones para extinción del fuego y procedimientos de evacuación,

b) instalaciones para prevención de inundaciones y procedimientos de evacuación,

c) procedimientos para manejo de bombas y procedimientos de evacuación relacionados,

d) investigadores especializados en fraude con sistemas de información y

e) investigadores especializados en ataques técnicos.

8.2.5 Análisis forenses de seguridad de la información

Cuando mediante una evaluación previa se identifica que el análisis forense de seguridad de la información se requiere con propósitos de evidencia, de hecho en el contexto de un incidente significativo de seguridad de la información, lo debería llevar a cabo el ISIRT. Debería involucrar el uso de técnicas y herramientas de investigación basadas en TI, apoyadas en procesos documentados, para revisar con más detalle el(los) incidentes de seguridad de la información designados, de lo que se ha revisado hasta ese momento en el proceso de gestión de incidentes de seguridad de la información. Se debería llevar a cabo de manera estructurada, y, si es pertinente, identificar qué se puede usar como evidencia, ya sea para procedimientos disciplinarios internos o acciones legales.

Los medios necesarios para el análisis forense de seguridad de la información es probable que sean clasificados como técnicos (por ejemplo, herramientas de auditoría, instalaciones para recuperación de evidencias), procedimentales, personal y oficinas seguras. Cada actividad de análisis forense de seguridad de la información se debería documentar completamente, e incluir las fotografías, reportes de análisis de registro de auditorías y registros de recuperación de datos, los que sean pertinentes. La competencia de la(s) persona(s) que lleva(n) a cabo el análisis forense de seguridad de la información debería estar documentada, junto con los registros de las pruebas de competencia. También es conveniente documentar cualquier otra información que demuestre la objetividad y naturaleza lógica del análisis. Todos los registros de los incidentes de seguridad de la información, de las actividades de análisis forense de seguridad de información, etc., y los medios asociados, se deberían almacenar en un ambiente seguro físicamente, y controlado por procedimientos que eviten que personal no autorizado tenga acceso a dichos registros y medios, los altere o los deje en un estado que no permita utilizarlos. Las herramientas basadas en TI para análisis forense de seguridad de la información deberían cumplir con estándares, de manera que su exactitud no se pueda impugnar legalmente, y se deberían mantener actualizados en línea con los cambios tecnológicos. El ambiente físico del ISIRT debería proporcionar condiciones demostrables que aseguren que la evidencia se maneja de manera que no es posible cuestionarla. Debería haber suficiente personal disponible de guardia, si es necesario, para poder responder en cualquier momento.

Con el tiempo, pueden surgir nuevos requisitos de examinar evidencia de una variedad de incidentes de seguridad de la información, incluido fraude, robo y vandalismo. De esta manera, para ayudar al ISIRT deben haber medios y procedimientos de soporte basados en TI, disponibles para revelar información oculta en un sistema, servicio o red de información, incluida información que en la inspección inicial parece que ha sido eliminada, encriptada o dañada. Estos medios deberían tener en cuenta todos los aspectos conocidos asociados con los tipos conocidos de incidentes de seguridad de la información y deberían estar documentados en los procedimientos del ISIRT.

En el ambiente de hoy, con frecuencia, el análisis forense de seguridad de la información es necesario para abarcar ambientes en red complejos, en donde es necesario que la investigación abarque un medio operativo completo, incluida una gran cantidad de servidores (por ejemplo, archivos, impresiones, comunicaciones y correos electrónicos) al igual que aplicaciones de acceso remoto. Hay muchas herramientas disponibles, incluidas las de búsqueda de texto, software de imágenes de disco y paquetes forenses de seguridad de la información. El enfoque principal de los procedimientos de análisis forense de seguridad de la información es asegurar que la evidencia se mantenga intacta y asegurarse de que resiste cualquier cuestionamiento legal. Se hace énfasis en que el análisis forense de seguridad de la información se debería llevar a cabo en una copia exacta de los datos originales, para evitar que el trabajo de análisis afecte la integridad del medio original. El proceso de análisis forense de seguridad de la información debería abarcar, en cuanto sea pertinente, las siguientes actividades:

a) Actividad para asegurar que el sistema, servicio y/o red que son el objetivo, estén protegidos durante el análisis forense de seguridad de la información, para no ser puestos en riesgo, alterados o dejados no disponibles, por la introducción de códigos maliciosos (incluidos virus), y que no haya efectos en las operaciones normales, o que sean mínimos.

b) Actividad para priorizar la adquisición y recolección de evidencia, es decir, de la más volátil a la menos volátil (esto depende en gran medida de la naturaleza del incidente de seguridad de la información).

c) Actividad para identificar todos los archivos pertinentes en el sistema, servicio y/o red, incluidos archivos normales, archivos con contraseña o protegidos de otra manera, y archivos encriptados.

d) Actividad para recuperar tanto como sea posible los archivos eliminados descubiertos, y otros datos.

e) Actividad para revelar direcciones IP, nombres de equipos, rutas de red e información de sitios web.

f) Actividad para extraer el contenido de archivos ocultos, temporales e intercambiados usados tanto por las aplicaciones como por el software del sistema operativo.

g) Actividad para ingresar al contenido de archivos protegidos o encriptados (a menos que lo impida a ley).

h) Actividad para analizar todos los datos posiblemente pertinentes encontrados en áreas de almacenamiento en disco especiales (y habitualmente inaccesibles).

i) Actividad para analizar los tiempos de acceso, modificación y creación de archivos.

j) Actividad para analizar los registros de las aplicaciones y sistemas/servicios/redes.

k) Actividad para determinar la actividad de los usuarios y/o aplicaciones en un sistema/servicio/red.

l) Actividad para analizar los correos electrónicos para obtener información sobre fuentes y contenidos.

m) Actividad para examinar la integridad de los archivos, con el fin de detectar archivos con troyanos y archivos que no estaban originalmente en el sistema.

n) Actividad para analizar, si es aplicable, evidencia física, por ejemplo, huellas, daño a la propiedad, videos de vigilancia, registros del sistema de alarma, registros de tarjetas de acceso y entrevistas a testigos.

o) Actividad para asegurar que la evidencia potencial extraída sea manejada y almacenada de manera que no sufra daño o quede inutilizable, y que el material confidencial no pueda ser visto por personas no autorizadas. Se hace énfasis en que la recolección de evidencia siempre debería estar de acuerdo con las reglas del tribunal o audiencia en la que se presente la evidencia.

p) Actividad para elaborar conclusiones sobre las razones para el incidente de seguridad de la información, las acciones requeridas y el tiempo para éstas, con evidencia que incluya listas de archivos pertinentes incluidos en un anexo al reporte principal.

q) Actividad para brindar soporte de expertos en caso de cualquier acción disciplinaria o legal, según se requiera.

Los métodos que se utilicen deberían estar documentados en los procedimientos del ISIRT.

El ISIRT debería contar con suficientes combinaciones de habilidades para brindar una cobertura amplia en cuanto a conocimiento técnico (incluidas las herramientas y técnicas que probablemente usen los atacantes), experiencia en análisis/investigación (incluida la

preservación de evidencia utilizable), conocimiento de la legislación pertinente y de las implicaciones de las reglamentaciones, y conocimiento regular sobre tendencias de incidentes.

Se debería reconocer lo siguiente:

a) es posible que algunas organizaciones no tengan recursos disponibles, y puede ser necesario contratar especialistas externos en análisis forense de seguridad de la información,

b) la recolección de material forense de seguridad de la información puede ser solamente un recurso (es decir, se justifican el esfuerzo y los gastos) donde ha ocurrido una pérdida grave o es probable que haya procedimientos penales, y

c) si no se usan recursos especializados para recolectar el material forense de seguridad la información es probable que los hallazgos no sean admisibles ni se requiriera una acción judicial.

8.2.6 Comunicaciones

En muchos casos en los que el ISIRT ha confirmado que un incidente de seguridad de la información es real, es necesario informar a determinadas personas, tanto interna (por fuera de las líneas de comunicación de la gerencia/ISIRT normales) como externamente, incluida la prensa. Es posible que esto sea necesario en varias etapas, por ejemplo, cuando se confirma que un incidente de seguridad de la información es real, cuando se confirma que está bajo control, cuando se designa para actividades de crisis, cuando se cierra y cuando se ha llevado a cabo completamente la revisión posterior al incidente y se han obtenido conclusiones.

Cuando las comunicaciones son necesarias, es conveniente tener cuidado para asegurar quién necesita saber qué, y en qué momento. Es conveniente determinar quiénes son las partes involucradas afectadas y preferiblemente dividirlas en grupos, tales como:

a) partes involucradas internas directas (gestión de crisis, personal de la gerencia, etc.),

b) partes involucradas externas directas (dueños, clientes, socios, proveedores, etc.), y

c) otros contactos externos, tales como la prensa y/u otros medios.

Cada grupo puede necesitar información especial que debería pasar a través de los canales adecuados de la organización. Una de las tareas de comunicación más importantes después de un incidente de seguridad de la información, es asegurarse de que las partes involucradas directas, tanto internas como externas recibirán la información, antes que sea transmitida a otros contactos externos, tales como la prensa.

Para ayudar a esta actividad cuando surja la necesidad, una práctica recomendable es preparar de antemano alguna información que se ajuste rápidamente a las circunstancias de un incidente particular de seguridad de la información y que se comunique a cada grupo pertinente y en particular a la prensa y/u otros medios. Si cualquier información concerniente a incidentes de seguridad de la información va a ser comunicada a la prensa, se debería hacer de acuerdo con la política de la organización acerca de divulgación de información. La información que se vaya a comunicar debería ser revisada por las partes pertinentes, que pueden incluir a la dirección, coordinadores de relaciones públicas y personal de seguridad de la información.

NOTA Las comunicaciones de incidentes de seguridad de la información pueden variar dependiendo del incidente y de su impacto, en combinación con las relaciones de la organización y su tipo de negocio. El tipo de negocio también puede establecer reglas específicas acerca de cómo deberían ser las comunicaciones, por ejemplo, si la organización está registrada en la bolsa de valores.

8.2.7 Escalamiento

En circunstancias extremas, es posible que los asuntos tengan que escalarse, para tratar asuntos que están fuera de control y existe el peligro potencial de un impacto inaceptable para el negocio. Estos incidentes necesitan escalarse para activar el plan de continuidad del negocio, si está implementado, mediante reporte a la dirección, a otro grupo dentro de la organización o a personas o grupos por fuera de ésta. Esto puede ser con el fin de que se tome una decisión sobre las acciones que se recomiendan para tratar un incidente de seguridad de la información o para una evaluación posterior para determinar qué acciones se requieren. Esto se puede llevar a cabo después de las actividades de evaluación descritas en los numerales 7.2 y 7.3, o durante estas actividades, si se hace evidente algún aspecto importante. Debería haber disponibles directrices en la documentación del esquema de gestión de incidentes de seguridad de la información para aquellos que probablemente en algún punto necesiten escalarse, es decir, los miembros del PoC (Punto de Contacto) o del ISIRT.

8.2.8 Registro de actividades y control de cambios

Se hace énfasis en que todos los involucrados en el reporte y gestión de un incidente de seguridad de la información deberían registrar adecuadamente todas las actividades para análisis posterior. Esto se debería incluir en el formulario de reporte de incidentes de seguridad de la información y en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, que se mantiene actualizada continuamente, durante todo el ciclo de un incidente de seguridad de la información, desde el primer reporte hasta la finalización de la revisión posterior al incidente.

Es conveniente que esta información se retenga en forma segura, de manera comprobable, y con un régimen adecuado de copias de respaldo. Además, todos los cambios hechos en el contexto del rastreo de un incidente de seguridad de la información y de actualización del formulario de reporte de incidentes de seguridad de la información y de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, deberían estar dentro de un esquema de control de cambios aceptado formalmente.

9. FASE DE LECCIONES APRENDIDAS

9.1 VISIÓN GENERAL DE LAS ACTIVIDADES CLAVE

La cuarta fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información se lleva a cabo, cuando los incidentes de seguridad de la información se han solucionado/cerrado, e involucra el aprendizaje de lecciones acerca de cómo los incidentes (y las vulnerabilidades se han manejado y tratado. Para la fase de lecciones aprendidas, una organización debería asegurar que las actividades clave sean las siguientes:

a) Actividad para llevar a cabo el análisis forense de seguridad de la información, según se requiera.

b) Actividad para identificar las lecciones aprendidas de incidentes y vulnerabilidades de seguridad de la información.

c) Actividad para revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información (controles nuevos y/o actualizados), al igual que la política de gestión de incidentes de seguridad de la información, como resultado de las lecciones aprendidas, ya sea de un incidente de seguridad de la información o de varios de ellos (o de las vulnerabilidades de seguridad de la información reportadas). A esto contribuye la métrica incluida en la estrategia de la organización, acerca de dónde invertir en los controles de seguridad de la información.

d) Actividad para revisar, identificar, y si es posible, hacer mejoras a los resultados de la revisión por la dirección y la evaluación de riesgos para la seguridad de la información existentes, como resultado de las lecciones aprendidas.

e) Actividad para examinar cómo fue la eficacia de los procesos, procesos, formularios de reporte y/o la estructura organizacional para responder a la evaluación y recuperación de cada incidente de seguridad de la información y tratar las vulnerabilidades de seguridad de la información, y con base en las lecciones aprendidas identificar y hacer mejoras en el esquema de gestión de incidentes de seguridad de la información y su documentación.

f) Actividad para actualizar de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

g) Actividad para comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si la organización lo desea).

Se hace énfasis en que las actividades de gestión de incidentes de seguridad de la información son repetitivas, y por tanto, la organización debería hacer mejoras regulares a varios elementos de seguridad de la información, en el tiempo. Estas mejoras se deberían proponer, con base en las revisiones de los datos sobre los incidentes de seguridad de la información y las respuestas a éstos, y de las vulnerabilidades de seguridad de la información reportadas, al igual que las tendencias en el tiempo.

9.2 ANÁLISIS FORENSE DE SEGURIDAD DE LA INFORMACIÓN ADICIONALES

Es posible que una vez que haya sido solucionado un incidente siga siendo necesario un análisis forense de seguridad de la información, para identificar evidencia. Éste lo debería llevar a cabo el ISIRT usando el mismo conjunto de herramientas y procedimientos sugeridos en el numeral 8.2.5.

9.3 IDENTIFICACIÓN DE LAS LECCIONES APRENDIDAS

Una vez que se haya cerrado un incidente de seguridad de la información, es importante que la organización identifique y aprenda rápidamente de las lecciones recibidas del manejo de un incidente de seguridad de la información, y que se asegure de que se actúa de acuerdo con las conclusiones. Además, puede haber lecciones por aprender de la evaluación y resolución de vulnerabilidades de seguridad de la información reportadas. Las lecciones pueden ser en los siguientes aspectos:

a) Requisitos nuevos o modificados para los controles de seguridad de la información. Estos controles pueden ser técnicos o de otro tipo (incluidos los físicos). Dependiendo de las lecciones aprendidas, éstas pueden incluir la necesidad de actualizaciones rápidas de los materiales, la entrega de las instrucciones de toma de conciencia sobre seguridad (para los usuarios, al igual que para otro personal), y una rápida actualización y publicación de directrices y/o normas.

b) La información nueva o modificada sobre vulnerabilidades y amenazas, y en consecuencia, los cambios en los resultados de la evaluación por la dirección y de la evaluación de riesgos de seguridad de la información existentes de la organización.

c) Cambios al esquema de gestión de incidentes de seguridad de la información y a sus procesos, procedimientos, los formularios de reporte y/o la estructura organizacional, y la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Una organización debería mirar más allá de un solo incidente o vulnerabilidad de seguridad de la información y revisar tendencias/patrones que puedan ayudar a identificar la necesidad de cambio en los controles o en los enfoques. También es recomendable, después del incidente de seguridad de la información orientado a TI, probar la seguridad, particularmente hacer una evaluación de vulnerabilidades. Así, una organización debería analizar regularmente los datos de la base de datos de eventos/incidentes/vulnerabilidades, con el fin de:

a) identificar tendencias/patrones,

b) identificar áreas de preocupación, y

c) analizar si se pueden llevar a cabo acciones preventivas para reducir la probabilidad de futuros incidentes.

La información obtenida durante un incidente de seguridad de la información se debería canalizar hacia un análisis de tendencias/patrones (en forma similar a como se manejan las vulnerabilidades de seguridad de información reportadas). Contribuye significativamente a la identificación temprana de incidentes de seguridad de la información y brinda una advertencia en cuanto a qué otros incidentes de seguridad de la información pueden ocurrir, con base en experiencias previas y en conocimiento documentado.

También se debería utilizar la información sobre incidentes de seguridad de la información y vulnerabilidades relacionadas provenientes del gobierno, los ISIRT comerciales y los proveedores.

Las pruebas de seguridad/evaluación/vulnerabilidades de un sistema, servicio y/o red de información posteriores a un incidente de seguridad de la información no se deberían confinar solamente al sistema, servicio y/o red de información afectados por el incidente de seguridad de la información. Se debería ampliar, de manera que se incluya cualquier sistema, servicio y/o red de información relacionada. Una evaluación completa de la vulnerabilidad se usa para resaltar la existencia de las vulnerabilidades aprovechadas durante el incidente de seguridad de la información en otros sistemas, servicios y/o redes, y para asegurar que no se introducen nuevas vulnerabilidades.

Es importante enfatizar que las evaluaciones de vulnerabilidad se deberían llevar a cabo regularmente, y que la reevaluación de vulnerabilidades después de que ocurre un incidente de seguridad de la información debería formar parte de este proceso de evaluación continua, no un reemplazo.

Se deberían elaborar resúmenes de los análisis de incidentes y vulnerabilidades de seguridad de la información, para tratar en cada reunión del foro de seguridad de información de la gerencia de la organización, y/u otros foros definidos en la política general de seguridad de información de la organización.

9.4 IDENTIFICACIÓN Y MEJORAS EN LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Durante la revisión llevada a cabo después de que se han solucionado uno o más incidentes o vulnerabilidades de seguridad de la información, se pueden identificar controles nuevos o modificaciones a éstos, según se requieran. Las recomendaciones y los requisitos de control relacionados pueden ser tales, que no sea viable financiera ni operativamente implementarlos de inmediato, en cuyo caso se deberían incluir en los objetivos de la organización a un plazo más largo. Por ejemplo, es posible que la migración a un cortafuego más seguro y robusto no sea viable financieramente a corto plazo, pero es necesario tenerla en cuenta en las metas a largo plazo de la organización para seguridad de la información.

De acuerdo con las recomendaciones acordadas, la organización debería implementar los controles actualizados o nuevos controles. Estos pueden ser controles técnicos (incluidos los físicos) y pueden incluir la necesidad de actualizaciones rápidas de los materiales, la entrega rápida de las instrucciones de toma de conciencia sobre seguridad (para los usuarios, al igual que para otro personal), y una rápida actualización y publicación de directrices y/o normas. Además, los sistemas, servicios y/o redes de información de la organización se deberían someter a evaluaciones regulares de vulnerabilidad para ayudar a identificar vulnerabilidades y brindar un proceso de afianzamiento continuo del sistema/servicio/red.

Además, aunque las revisiones de procedimientos y documentación relacionados con seguridad de la información se pueden llevar a cabo en forma inmediata después de un incidente de seguridad de la información o de una vulnerabilidad resuelta, es más probable que se requiera como una respuesta posterior. Después de un incidente de seguridad de la información o de una vulnerabilidad resuelta, si es pertinente, una organización debería actualizar sus políticas y procedimientos de seguridad de la información para tener en cuenta la información recolectada, y cualquier problema identificado durante el curso del proceso de gestión de incidentes. Una meta a largo plazo del ISIRT debería ser, junto con el líder de seguridad de la información de la organización, asegurar que tanto la política de seguridad de la información como las actualizaciones de los procedimientos, se divulguen en toda la organización.

9.5 IDENTIFICACIÓN Y MEJORAS A LOS RESULTADOS DE LA REVISIÓN POR LA DIRECCIÓN Y DE LA EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Dependiendo de la severidad y del impacto de un incidente de seguridad de la información (o la severidad y el impacto potencial relacionado con una vulnerabilidad de seguridad de la información reportada), puede ser necesaria una evaluación de los resultados de la evaluación por la dirección y de la evaluación de riesgos de seguridad de la información para tener en cuenta nuevas amenazas y vulnerabilidades. Como continuación a la realización de la revisión por la dirección y la evaluación actualizada de riesgos de seguridad de la información, puede ser necesario introducir cambios o nuevos controles (véase el numeral 9.4).

9.6 IDENTIFICACIÓN Y MEJORAS EN EL ESQUEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Posteriormente a la resolución de un incidente, el líder del ISIRT o la persona designada debería examinar todo lo sucedido y cuantificar la eficacia de la respuesta entera a un incidente de seguridad de la información. Este análisis busca determinar qué partes del esquema de gestión de incidentes de seguridad de la información funcionaron con éxito, e identificar si se requiere alguna mejora.

Un aspecto importante del análisis posterior a su respuesta es retroalimentar información y conocimiento al esquema de gestión de incidentes de seguridad de la información. Si son de una gravedad suficiente, la organización se debería asegurar de que se programe una reunión entre las partes pertinentes, poco después de la resolución del incidente, mientras la información está aún fresca en la mente de las personas. Los factores por considerar en esta reunión incluyen los siguientes:

a) ¿Los procedimientos establecidos en el esquema de gestión de incidentes de seguridad de la información funcionaron en la forma prevista?

b) ¿Hay algunos procedimientos o métodos que habrían ayudado a la detección del incidente?

c) ¿Se identificaron algunos procedimientos o herramientas que habrían sido de ayuda en el proceso de respuesta?

d) ¿Hubo algunos procedimientos que hubieran ayudado a la recuperación de los sistemas de información después de que se identificó el incidente?

e) ¿La comunicación del incidente a todas las partes pertinentes fue eficaz durante todo el proceso de detección, reporte y respuesta?

Los resultados de la reunión se deberían documentar. La organización se debería asegurar de que se examinan las áreas identificadas para la mejora del esquema de gestión de incidentes de seguridad de la información, y de que los cambios justificados se incorporan a una actualización de la documentación del esquema. Los cambios en los procesos, procedimientos y los formularios de reporte de gestión de incidentes de seguridad de la información se deberían someter a una revisión y probar en forma minuciosa antes de su implementación.

9.7 OTRAS MEJORAS

Se pueden haber identificado otras mejoras durante la fase de lecciones aprendidas, por ejemplo, cambios en las políticas, normas y procedimientos de seguridad de la información, y cambios en el hardware de TI y en las configuraciones del software. La organización se debería asegurar de que se implementen.

ANEXO A
(Informativo)

Tabla de referencias cruzadas entre la NTC-ISO/IEC 27001 y la GTC-ISO/IEC 27035

Numeral NTC-ISO/IEC 27001:2005	Numeral GTC-ISO/IEC 27035
4.2.2 Implementación y operación del SGSI La organización debe: h. implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad (véase numeral 4.2.3).	4 (Visión general) para la visión general de la implementación de la gestión de incidentes de seguridad de la información. 5 (Planificación y preparación). El contenido puede ayudar a implementar la gestión de incidentes de seguridad de la información. 6 (Detección y reporte) 7 (Evaluación y decisión), 8 (Respuestas) y 9 (Lecciones aprendidas). El contenido puede ayudar a llevar a cabo la gestión de incidentes de seguridad de la información.
4.2.3 Seguimiento y revisión del SGSI La organización debe: a) Ejecutar procedimientos de seguimiento y revisión y otros controles para: 2) Identificar con prontitud los **incidentes** e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron. 4) Ayudar a detectar eventos de seguridad, y de esta manera, impedir **incidentes** de seguridad mediante el uso de indicadores. b) Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad), teniendo en cuenta los resultados de las auditorías de seguridad, **incidentes**, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.	9 (Lecciones aprendidas). El contenido puede ayudar a hacer el seguimiento y la revisión de la gestión de incidentes de seguridad de la información.
4.3.3 Control de registros Se deben llevar registros del desempeño del proceso, como se esboza en el numeral 4.2, y de todos los casos de **incidentes** de seguridad significativos relacionados con el SGSI.	5.1 (Visión general de las actividades clave), 6 (Detección y reporte), y Anexo D (Ejemplo de evento de seguridad de la información, reportes y formularios de incidentes y vulnerabilidades). El contenido puede ayudar a definir el alcance de los registros.
A.13 Gestión de incidentes de seguridad de la información	4 (Visión general) para la visión general de la implementación de la gestión de incidentes de seguridad de la información. 5 (Planificación y preparación). El contenido puede ayudar a implementar la gestión de incidentes de seguridad de la información.

Numeral NTC-ISO/IEC 27001:2005	Numeral GTC-ISO/IEC 27035
A.13.1 Reporte sobre los eventos y vulnerabilidades de seguridad de la información Objetivo: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente. Debería haber implementados procedimientos formales de reporte y escalamiento de los eventos. Todos los empleados, contratistas y usuarios de terceras partes deberían tener conocimiento de los procedimientos para reportar diferentes tipos de eventos y vulnerabilidades que pueden tener impacto en la seguridad de los activos de la organización. Se les debería exigir que reporten eventos y vulnerabilidades de seguridad de la información tan pronto como sea posible, al PoC (Punto de Contacto) designado. **A.13.1.1 Reporte sobre los eventos de seguridad de la información** Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. **A.13.1.2 Reporte sobre las debilidades de seguridad** Control: Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información, que observen y reporten todas las debilidades observadas o sospechosas en los sistemas o servicios.	5 (Planificar y preparar) (en particular, véase 5.4 Esquema de gestión de incidentes de seguridad de la información, 5.5 Establecimiento del ISIRT, 5.6 Soporte técnico y otro, 5.7 Toma de conciencia y formación, y 5.8 Prueba de los esquemas), 6 (Detección y reporte), Anexo C (Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información) y Anexo D (Ejemplo de reportes y formularios de eventos, incidentes y vulnerabilidades de seguridad de la información). El contenido puede ayudar a reportar eventos y vulnerabilidades de seguridad de la información. Anexo D.2.1 (Ejemplo de elementos del registro para el evento de seguridad de la información) para el ejemplo del formulario de reporte. Anexo D.2.3 (Ejemplo de elementos del registro para vulnerabilidades de seguridad de la información) y el Anexo D.4.3 (ejemplo de formulario para reporte de vulnerabilidades de seguridad de la información) para el ejemplo del formulario de reporte.
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información. Debería haber implementados responsabilidades y procedimientos para manejar eficazmente eventos y vulnerabilidades de seguridad de la información una vez que se hayan reportado. Se debería aplicar un proceso de mejora continua a la respuesta, seguimiento, evaluación y gestión global de incidentes de seguridad de la información. Cuando se requiere evidencia, ésta se debería recolectar para asegurar conformidad con los requisitos legales. **A.13.2.1 Responsabilidades y procedimientos** Control: Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	7 (Evaluación y decisión), 8 (Respuestas), y 9 (Lecciones aprendidas), y el Anexo B (Ejemplo de incidentes de seguridad de la información y sus causas), Anexo C (Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información) y el Anexo E (Aspectos legales y reglamentarios). 7 (Evaluación y decisión), 8 (Respuestas), Anexo D.2.2 (Elementos de ejemplo del registro para incidentes de seguridad de la información) y el Anexo D.4.2 (Formulario de ejemplo para el reporte de incidentes de seguridad de la información). El contenido puede ayudar a definir las responsabilidades y procedimientos.

Numeral NTC-ISO/IEC 27001:2005	Numeral GTC-ISO/IEC 27035
A.13.2.2 Aprendizaje debido a los incidentes de seguridad de la información Control: Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de incidentes de seguridad de la información. **A.13.2.3 Recolección de evidencia** Control: Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	9 (Lecciones aprendidas) y Anexo B (Ejemplo de incidentes de seguridad de la información y sus causas), y Anexo C (Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información). El contenido puede ayudar a aprender de los incidentes de seguridad de la información. 7 (Evaluación y decisión), 8 (Respuestas) (en particular, véase el numeral 8.2.5 Análisis forense de seguridad de la información) y el Anexo E (Aspectos legales y reglamentarios). El contenido puede ayudar a definir los procedimientos para la recolección de evidencia.

ANEXO B
(Informativo)

EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y SUS CAUSAS

B.1 ATAQUES

B.1.1 Denegación de servicio

La denegación de servicio (siglas en inglés: DoS) y denegación de servicio distribuida (siglas en inglés: DDoS) son una amplia categoría de incidentes con un denominador común. Estos incidentes hacen que un sistema, servicio o red dejen de operar a su capacidad prevista, con mucha frecuencia con la denegación completa de acceso a usuarios legítimos. Existen dos tipos de incidentes DoS/DDoS causados por medios técnicos: eliminación y agotamiento de recursos.

Algunos ejemplos típicos de incidentes DoS/DDoS deliberados incluyen:

- envío masivo de paquetes TCP para llenar el ancho de banda de red con tráfico de respuesta,

- envío de datos en un formato inesperado, a un sistema, servicio o red, con la intención de hacerlo colapsar o interrumpir su operación normal y

- apertura de múltiples sesiones autorizadas con un sistema, servicio o red particular, con la intención de agotar sus recursos (es decir, retardarlo, bloquearlo o hacerlo colapsar).

Estos ataques se realizan con frecuencia por medio de *botnets*, un grupo de robots de software (códigos maliciosos) que funcionan en forma autónoma y automática. Los *botnets* pueden comunicarse con centenares o millones de computadores afectados.

Algunos incidentes técnicos de denegación de servicio pueden ser causados accidentalmente, por ejemplo, una configuración equivocada hecha por un operador o por incompatibilidad del software de la aplicación, pero la mayoría de veces son deliberados. Algunos incidentes técnicos de denegación de servicio se hacen intencionalmente para hacer colapsar un sistema o servicio, o hacer colapsar una red, mientras que otros son apenas las consecuencias de otras actividades maliciosas. Por ejemplo, algunas de las técnicas de identificación y escaneo sigilosos más comunes pueden causar que los sistemas o servicios más antiguos o mal configurados colapsen cuando son escaneados. Es conveniente observar que muchos incidentes de denegación de servicio deliberados con frecuencia se ejecutan en forma anónima (es decir, la fuente del ataque es “falsa”), ya que habitualmente no dependen de que el atacante reciba información de la red o sistema atacados.

Los incidentes de denegación de servicio causados por medios no técnicos, que dan como resultado pérdida de información, servicios y/o aplicaciones pueden ser causados por (ejemplos):

- violaciones a las medidas de seguridad físicas, dando como resultado robo o daño intencionado y destrucción de equipos;

- daño accidental al hardware (y al lugar en que se encuentra) por incendio o daño por agua/inundación;

- condiciones ambientales extremas, por ejemplo, altas temperaturas de operación (por ejemplo, debido a fallas en el aire acondicionado);

- mal funcionamiento de sistemas, o sobrecarga;

- cambios no controlados en el sistema, y

- mal funcionamiento en el software o hardware.

B.1.2 Acceso no autorizado

En general, esta categoría de incidentes consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Algunos ejemplos de incidentes de acceso no autorizado provocados técnicamente incluyen:

- intentos por recuperar archivos de contraseñas;

- ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo (por ejemplo, administrador del sistema);

- aprovechamiento de las vulnerabilidades del protocolo para secuestrar o dirigir equivocadamente las conexiones de red legítimas, e

- intentos de elevar privilegios a recursos o información más allá de los que un usuario o administrador ya posee legítimamente.

Los incidentes de acceso no autorizado causados por medios no técnicos, que dan como resultado la divulgación o modificación directa o indirecta de información, carencias en la rendición de cuentas, o mala utilización de servicios de información, pueden ser causados por (ejemplos):

- violaciones a las medidas de seguridad física, que dan como resultado acceso no autorizado a la información y

- sistemas operativos mal configurados o que operan, en forma deficiente, debido a cambios no controlados en el sistema, o mal funcionamiento del software o del hardware.

B.1.3 Códigos maliciosos

Los códigos maliciosos identifican un programa o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, destrucción de información y de recursos, denegación de servicio, correo basura (*spam*), etc. Los ataques con códigos maliciosos se pueden subdividir en cinco categorías: virus, gusanos, troyanos, códigos móviles y combinaciones de estos. Aunque hace algunos años los virus se crearon para atacar cualquier sistema infectado vulnerable, en la actualidad los códigos maliciosos se usan para realizar ataques dirigidos. Esto se hace algunas veces modificando un código malicioso existente, creando una variante que muchas veces no reconocen las tecnologías para detección de códigos maliciosos.

B.1.4 Uso inadecuado

Este tipo de incidentes ocurre cuando un usuario viola las políticas de seguridad del sistema de información de la organización. Estos incidentes no son ataques en el sentido estricto de la palabra, pero con frecuencia se reportan como incidentes y los debería gestionar el ISIRT. Un uso inadecuado puede ser:

- descargar e instalar herramientas para piratería informática;
- usar el correo corporativo para correo basura o para la promoción de negocios personales;
- usar recursos corporativos para crear un sitio web no autorizado y
- usar actividades entre colegas para adquirir o distribuir archivos piratas (música, video, software).

B.2 RECOLECCIÓN DE INFORMACIÓN

En términos generales, la categoría de incidentes de recolección de información incluye las actividades asociadas con la identificación de objetivos potenciales y la comprensión de los servicios que funcionan en dichos objetivos. Este tipo de incidente involucra reconocimiento, en donde la meta es identificar:

- la existencia de un objetivo y comprender la topología de la red circundante, y con quién se comunica rutinariamente el objetivo, y
- las vulnerabilidades potenciales en el objetivo o en ambiente de red inmediata, que pudieran ser aprovechadas.

Algunos ejemplos típicos de ataques para recolección de información por medios técnicos incluyen:

- volcado de registros de Sistema de Nombre de Dominio para el dominio de internet del objetivo (zona de transferencia del DNS);
- envío masivo de paquetes TCP para encontrar sistemas que estén "activos";
- sondeo del sistema para identificar (por ejemplo, la huella) el sistema operativo del equipo;
- escaneo de los puertos de red disponibles en un sistema para identificar los servicios relacionados (por ejemplo, correo electrónico, FTP. Web, etc.) y la versión del software de estos servicios, y
- escaneo de uno o más servicios que se conoce que son vulnerables, a través de un rango de direcciones de red (escaneo horizontal).

En algunos casos, la recolección de información técnica se extiende a acceso no autorizado si, por ejemplo, como parte de la búsqueda de vulnerabilidades el atacante también intenta obtener acceso no autorizado. Esto ocurre comúnmente con herramientas de piratería informática automatizadas que no solamente buscan vulnerabilidades sino que también

intentan automáticamente aprovecharse de los sistemas, servicios y/o redes vulnerables que encuentra.

Los incidentes de recolección de información causados por medios no técnicos, que dan como resultado:

- divulgación o modificación directa o indirecta de información,
- robo de propiedad intelectual almacenada electrónicamente,
- carencias en la rendición de cuentas, por ejemplo, en el acceso a cuentas y
- mal uso de los sistemas de información (por ejemplo, contrario a la ley o a la política de la organización),

pueden ser causados, entre otros, por:

- violaciones a las medidas de seguridad física, que dan como resultado acceso no autorizado a información, y robo de equipos para almacenamiento de datos que contienen datos importantes, por ejemplo, claves de encriptación, o
- sistemas operativos mal configurados o configurados en forma deficiente debido a cambios no controlados en el sistema, o mal funcionamiento del hardware o software, que da como resultado personal interno o externo que obtiene acceso a información para la que no está autorizado.

ANEXO C
(Informativo)

EJEMPLO DE ENFOQUES PARA LA CATEGORIZACIÓN Y CLASIFICACIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

C.1 INTRODUCCIÓN

Este anexo presenta ejemplos de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Estos enfoques posibilitan que el personal y las organizaciones documenten los incidentes de seguridad de la información, de manera consistente, que permite obtener los siguientes beneficios:

- promover que se intercambie y comparta la información sobre incidentes de seguridad de la información,
- facilitar el reporte de incidentes de seguridad de la información y las respuestas a éstos,
- mejorar la eficiencia y eficacia del manejo y gestión de incidentes de seguridad de la información,
- facilitar la recolección y el análisis de datos sobre incidentes de seguridad de la información, e
- identificar los niveles de severidad de los incidentes de seguridad de la información usando un criterio consistente.

Estos ejemplos de enfoques para la categorización y clasificación también se pueden aplicar a eventos de seguridad de la información, pero no comprenden las vulnerabilidades de seguridad de la información.

C.2 CATEGORIZACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información pueden ser causados por acciones humanas deliberadas o accidentales y también por medios técnicos o físicos. El siguiente enfoque caracteriza los incidentes de seguridad de la información considerando las amenazas como factores de categorización (en relación con amenazas, véase la ISO/IEC 27005:2008, Anexo C, Ejemplo de amenazas típicas). En la Tabla C.1 se presenta una lista de categorías de incidentes de seguridad de la información.

Tabla C.1. Categorías de incidentes de seguridad de la información, de acuerdo con las amenazas

Categoría	Descripción	EJEMPLOS
Incidente de desastre natural	La pérdida de seguridad de la información es causada por desastres naturales que están por fuera del control humano.	Terremotos, volcanes, inundaciones, ciclones, rayos, tsunamis, derrumbes, etc.
Incidente de disturbios sociales	La pérdida de seguridad de la información es causada por la inestabilidad de la sociedad.	ataque terrorista, guerra, etc.
Incidente de daño físico	La pérdida de seguridad de la información es causada por acciones físicas accidentales o deliberadas.	Incendio, agua, electrostática, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de equipos, destrucción de medios, robo de equipos, robo de medios, pérdida de equipos, pérdida de medios, alteración de equipos, alteración de medios, etc.
Incidente de fallas de infraestructura	La pérdida de seguridad de la información es causada por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información.	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, en el suministro de agua, etc.
Incidente de perturbación por radiaciones	La pérdida de seguridad de la información es causada por perturbaciones debidas a radiaciones.	Radiación electromagnética, pulsos electromagnéticos, interferencia electrónica, fluctuación de tensión, radiación térmica, etc.
Incidente de falla técnica	La pérdida de seguridad de la información es causada por fallas en los sistemas de información o en instalaciones no técnicas relacionadas, al igual que problemas humanos no intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de información.	Falla del hardware, mal funcionamiento del software, sobrecarga (saturación de la capacidad de los sistemas de información), violación de la mantenibilidad, etc.

Continúa...

Tabla C.1. (Continuación)

Categoría	Descripción	EJEMPLOS
Incidente de *malware*	La pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, la integridad o disponibilidad de los datos, las aplicaciones o sistemas operativos, y/o afectar la operación normal de los sistemas de información.	Virus informáticos, gusanos de red, troyanos, *botnet*, ataques combinados, páginas web con códigos maliciosos, sitio *hosting* con códigos maliciosos, etc. Un virus informático es un conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador. A diferencia de los programas normales, tiene capacidad de autoreplicación y usualmente porta una carga útil que puede afectar las operaciones del computador o destruir los datos. A diferencia de un virus informático, un gusano de red es un tipo de programa malicioso que se autodisemina y autorreplica automáticamente, a través de las redes, aprovechando las vulnerabilidades de los sistemas de información en las redes. Un troyano es un tipo de programa malicioso disfrazado de funciones inofensivas en los sistemas de información, y con capacidad para posibilitar que el autor controle los sistemas de información, incluido el robo o la interceptación de información de los sistemas. Un *botnet* es un grupo de computadores reclutados (zombis) en redes, controlados centralmente por el autor del *botnet*, quien se conoce como el controlador de *botnet*. Los *botnets* se forman deliberadamente al infectar masivamente los computadores en redes con programas *bot*. Los *botnets* se pueden usar para ataques oportunistas en redes, robo de información y diseminación de troyanos, gusanos de red y otros programas maliciosos. Los ataques combinados también pueden tener características combinadas de virus informáticos, gusanos de red, troyanos o *botnets*, etc. Los ataques combinados también pueden ser causados por operaciones combinadas de una serie de diferentes programas maliciosos. Por ejemplo, un virus informático o un gusano de red se introduce en el sistema informático y luego instala un troyano en el sistema. Una página web con un código malicioso embebido, corrompe el sitio web mediante la inclusión de un código malicioso (*malware)* en el sistema de un computador que ingresa a ella. Un sitio de alojamiento de un código malicioso mimetiza un código malicioso que es descargado por los usuarios objetivo.

Tabla C.1. (Continuación)

Categoría	Descripción	EJEMPLOS
Incidente de ataque técnico	La pérdida de seguridad de la información es causada por el ataque a sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones presentes del sistema.	Escaneo de redes, aprovechamiento de las vulnerabilidades, aprovechamiento de puertas traseras, intentos de ingreso, interferencia, denegación de servicio, etc. El escaneo de redes utiliza software con este fin, para adquirir información acerca de las configuraciones de red, puertos, servicios y vulnerabilidades existentes. Mediante el aprovechamiento de las vulnerabilidades se aprovechan y se utilizan los defectos del sistema de información, tales como configuraciones, protocolos o programas. Aprovechamiento de puertas traseras, que hace referencia al uso de éstas o de programas peligrosos dejados en los procesos de diseño de sistemas de software y de hardware. Intentos de adivinar, romper o forzar contraseñas. Interferencia que obstruye las redes de computador, las redes de radio y televisión con cableado o inalámbricas, o señales de radio y televisión satelital, a través de medios técnicos. La denegación de servicio es causada por el uso voraz de recursos de red y de sistemas de información tales como CPU, memoria, espacio en disco o ancho de banda de red, y de esta manera afecta la operación normal de los sistemas de información, por ejemplo, SYS-a, inundación de paquetes TCP y bombas a los correos electrónicos.
Incidente de violación de reglas	La pérdida de seguridad de la información es causada por violación de las reglas en forma accidental o deliberada.	Uso no autorizado de recursos, violación de los derechos de autor, etc. Uso no autorizado de recursos, recursos de acceso para propósitos no autorizados, incluidas agrupaciones temporales para la obtención de utilidades, por ejemplo, el uso del correo electrónico para participar en cadenas ilegales o esquemas de pirámide con fines lucrativos. La violación de derechos de autor es causada por la venta e instalación de copias de software sin licencia, u otros materiales protegidos por derechos de autor, por ejemplo, los warez.
incidente de compromiso de las funciones	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o deliberada las funciones de los sistemas de información en cuanto a seguridad.	Abuso de derechos, falsificación de derechos, denegación de acciones, operaciones equivocadas, violación de la disponibilidad de personal, etc. Abuso de derechos: uso de derechos más allá de los términos de referencia. Falsificación de derechos: se establecen falsos derechos con el fin de engañar. La denegación de acciones: se presenta cuando alguien niega lo que ha hecho. Las operaciones equivocadas: consisten en la realización de operaciones en forma incorrecta o no intencional. La violación en cuando a disponibilidad de personal: es causada por la falta o ausencia de recursos humanos.

Tabla C.1. (Final)

Categoría	Descripción	Ejemplos
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o deliberada la seguridad de la información, por ejemplo, en cuanto a confidencialidad, integridad, disponibilidad, etc.	Interceptación, espionaje, "chuzada" de teléfonos, divulgación, enmascaramiento, ingeniería social, *phishing* de redes, robo de datos, pérdida de datos, alteración de datos, errores de datos, análisis de flujo de datos, detección de posición, etc. Con la interceptación se capturan datos antes de que puedan llegar a los usuarios previstos. Espionaje es la recolección secreta de información y la divulgación de ésta acerca de las actividades de otra organización. "Chuzar" consiste en escuchar una conversación de una parte externa sin que ésta tenga conocimiento. Divulgación es hacer conocer públicamente información confidencial. Enmascaramiento es cuando una entidad simula ser otra. Ingeniería social consiste en la recolección de información de una persona utilizando medios no técnicos, por ejemplo, mentiras, trampas, sobornos o amenazas. *Phishing* de redes consiste en hacer uso de tecnología fraudulenta de redes de computador para convencer a los usuarios para que divulguen información importante, tal como detalles de cuentas bancarias de usuarios y contraseñas, mediante el uso de correos electrónicos engañosos. Robo de datos. Consiste en tomar datos sin autorización. Alteración de datos consiste en entrar en contacto con datos o hacerles cambios sin autorización. Error de datos es cometer errores cuando se ingresan o procesan datos. Detección de posición consiste en detectar la posición de información o sistemas confidenciales.
Incidente relacionado con contenidos peligrosos	La pérdida de seguridad de la información es causada por la propagación de contenido indeseable a través de redes de información, lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos.	Contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, etc. Contenido ilegal: es contenido publicado que viola las constituciones nacionales o internacionales, las leyes y las reglamentaciones, por ejemplo, pornografía infantil, exaltación de la violencia, falsificación, fraude. Contenido que provoca pánico: es la exposición sensacionalista maliciosa en Internet, sobre asuntos delicados, que da como resultado alteración social o pánico. Contenido malicioso: hace referencia a la difusión de contenido que ataca en forma maliciosa a personas o a la sociedad, por ejemplo, bromas pesadas y acoso. Contenido abusivo hace referencia a la transmisión de contenido que no ha sido aceptado por los receptores, por ejemplo, el correo masivo no autorizado.
Otros incidentes	No clasificados en ninguna de las categorías de incidentes anteriores.	

C.3 CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A continuación se presentan dos ejemplos de enfoques para clasificar los incidentes de seguridad de la información:

Se hace énfasis en que son ejemplos. Existen otros, como el FIRST / *Mitre Common Vulnerability Scoring System* (CVSS) y el UK *Government Structured Warning Information Format* (SWIF).

C.3.1 Ejemplo de enfoque 1

C.3.1.1 Factores de clasificación

C.3.1.1.1 Introducción

Este enfoque clasifica los incidentes de seguridad de la información considerando los tres factores siguientes:

- importancia del sistema de información,
- pérdida del negocio y
- impacto social.

C.3.1.1.2 Importancia del sistema de información

La importancia de los sistemas de información afectados por incidentes de seguridad de la información se determina considerando la importancia de las operaciones del negocio de la organización apoyados por sistemas de información. La importancia se puede expresar en relación con la seguridad nacional, el orden social, el desarrollo económico y el interés público, y la dependencia del negocio de los sistemas de información. Este enfoque clasifica la importancia de los sistemas de información en tres niveles amplios: sistema de información especialmente importante, sistema de información importante, y sistema de información común.

C.3.1.1.3 Pérdida del negocio

La pérdida del negocio de la organización, causada por incidentes de seguridad de la información, se determina considerando la severidad del impacto de la interrupción del negocio debido a daño del hardware/software, funciones y datos de los sistemas de información. La severidad del impacto puede depender del costo de llevar el negocio nuevamente a operación normal, y de otros efectos negativos de los incidentes de seguridad de la información, incluidas la pérdida de utilidades y/u oportunidades. Este enfoque clasifica la pérdida de negocios en cuatro niveles: pérdida del negocio especialmente grave, pérdida del negocio grave, pérdida del negocio considerable, y pérdida menor del negocio, como se describen a continuación:

a) Una pérdida del negocio especialmente grave significaría parálisis grande en el negocio, hasta el punto de hacerle perder la capacidad del negocio, y/o daño muy grave a la confidencialidad, integridad y disponibilidad de datos clave del negocio. Tendría un costo enorme llevar nuevamente el negocio a la normalidad y eliminar los efectos negativos. Una organización no puede soportar este nivel de pérdida del negocio.

b) Una pérdida del negocio grave significaría la interrupción de las operaciones del negocio durante un tiempo prolongado, o la parálisis local del negocio hasta el punto de influir gravemente en la capacidad del negocio, y/o causar daño grave a la

confidencialidad, integridad y disponibilidad de datos clave del negocio. Tendría un costo enorme llevar nuevamente el negocio a la normalidad y eliminar los efectos negativos. Una organización puede soportar este nivel de pérdida del negocio.

c) Una pérdida del negocio considerable significaría la interrupción en las operaciones del negocio, hasta el punto de influir considerablemente en la capacidad de negocio, y/o causar daño considerable a la confidencialidad, integridad y disponibilidad de datos importantes del negocio. Tendría un costo considerable llevar nuevamente el negocio a la normalidad y eliminar los efectos negativos. Una organización puede soportar completamente este nivel de pérdida del negocio.

d) Una pérdida menor del negocio significaría la interrupción en las operaciones del negocio durante un período corto, hasta el punto de influir de alguna manera en la capacidad del negocio, y/o causar impacto menor a la confidencialidad, integridad y disponibilidad de datos importantes del negocio. Tendría un costo menor llevar nuevamente el negocio a la normalidad y eliminar los efectos negativos.

C.3.1.1.4 Impacto social

El impacto en la sociedad causado por incidentes de seguridad de la información se determina considerando la escala y el grado de impacto sobre la seguridad nacional, el orden social, el desarrollo económico y el interés público. Este enfoque clasifica el impacto social en cuatro niveles: impacto social especialmente importante, impacto social importante, impacto social considerable, e impacto menor, como se describen a continuación:

I. Un impacto social especialmente importante significaría efectos adversos que abarcan la mayoría de áreas de una o más provincias/estados, que representa una gran amenaza para la seguridad nacional, causa alteración social, provoca consecuencias extremadamente adversas sobre el desarrollo económico y/o afecta seriamente el interés público.

II. Un impacto social importante significaría efectos adversos que abarcan la mayoría de áreas de una o más ciudades, que representa una amenaza para la seguridad nacional, causa pánico social, provoca consecuencias adversas significativas sobre el desarrollo económico y/o afecta el interés público.

III. Un impacto social considerable significaría efectos adversos que abarcan la mayoría de áreas de una o más ciudades, con amenaza limitada para la seguridad nacional, con alguna alteración del orden social, que provoca algunas consecuencias adversas sobre el desarrollo económico y/o afecta el interés público.

IV. Un impacto social menor significaría efectos adversos en parte de un área de una ciudad, una pequeña posibilidad de amenaza para la seguridad nacional, el orden social, el desarrollo económico y el interés público, pero con daño a los intereses de individuos, empresas y otras organizaciones.

C.3.1.2 Clases

C.3.1.2.1 Introducción

Con base en los factores de clasificación, los incidentes de seguridad de la información se deberían clasificar por severidad usando una escala. Esta escala puede ser sencilla, en la que se establezca “mayor” y “menor”, o más detallada, como se indica a continuación:

- Emergencia: impacto severo

- Crítica: Impacto medio

- Advertencia: impacto bajo

- Información: no hay impacto, pero el análisis se puede usar para mejorar las políticas, procedimientos o controles de seguridad de la información.

De acuerdo con los factores de clasificación anteriores, este enfoque clasifica los incidentes de seguridad de la información en cuatro clases:

- Muy grave (clase IV)

- Grave (clase III)

- Menos grave (Clase II)

- Pequeño (clase I)

Se hace énfasis en que estas clases de severidad son ejemplos. En algunos enfoques, la clase más grave está representada en el nivel más alto de la escala, mientras que en otros, la clase más grave está representada en el nivel más bajo de la escala.

C.3.1.2.2 Muy grave (Clase IV)

Incidentes muy graves son aquellos que

a) actúan sobre sistemas de información especialmente importantes,

b) dan como resultado pérdidas para el negocio especialmente graves, y

c) conducen a un impacto social especialmente importante.

C.3.1.2.3 Grave (Clase III)

Incidentes graves son aquellos que

a) actúan sobre sistemas de información especialmente importantes, o sistemas de información importantes, y

b) dan como resultado pérdidas graves para el negocio, o

c) conducen a un impacto social importante.

C.3.1.2.4 Clase menos grave (Clase II)

Incidentes menos graves son aquellos que

a) actúan sobre sistemas de información importantes o sistemas de información comunes, y

b) dan como resultado pérdidas considerables para el negocio, o

c) conducen a impacto social considerable.

C.3.1.2.5 Pequeños (Clase I)

Incidentes pequeños son aquellos que

a) actúan sobre sistemas de información importantes comunes,

b) dan como resultado pérdidas menores para el negocio o ninguna pérdida,

c) conducen a impactos sociales menores o a ningún impacto social y

d) no se requieren acciones y no hay consecuencias.

C.3.1.3 Categoría de incidentes y clase de severidad

La categoría de incidentes de seguridad de la información y la clase de severidad con frecuencia están relacionadas. Una categoría de incidentes de seguridad de la información puede tener diferentes clases de severidad, dependiendo no solamente del negocio sino también de la naturaleza del incidente de seguridad de la información tales como:

a) intencional,

b) dirigido,

c) temporizado y

d) masivo.

En la Tabla 2 se presentan algunos ejemplos de categorías de incidentes de seguridad de la información que pueden tener diferentes clases de severidad.

Tabla C.2 Ejemplos de categorías de incidentes y clases de severidad

Clase de severidad / Categoría de incidentes	Pequeña	Menos grave	Grave	Muy grave
Ataques Técnicos	Intentos fallidos	Único y común (Usuario comprometido)	Múltiple (Usuario comprometido) O uno importante importancia única Aplicación, o administración comprometidos)	Masivo (Aplicación, o administrador comprometido)
Ataques Técnicos		Molestia (Incidencia superficial)	Perturbación (Impacto en el rendimiento)	No disponibilidad (Detención de los servicios)
Malware (código malicioso)	Uno solo conocido (Detectado y bloqueado por la protección antivirus)	Uno solo desconocido	Múltiples infecciones Infecciones en el servidor	Infecciones masivas

C.3.2 Ejemplo de enfoque 2

C.3.2.1 Introducción

Este enfoque presenta ejemplos de directrices para evaluar las consecuencias adversas de los incidentes de seguridad de la información, en donde cada directriz usa una escala de 1 (bajo) a 10 (alto) para clasificar los incidentes de seguridad de la información. En la práctica, se pueden usar otras escalas, por ejemplo de 1 a 5, y cada organización debería adoptar la que mejor se ajuste a su entorno).

Antes de leer las directrices que se presentan más abajo, es conveniente tener en cuenta los siguientes puntos:

- En algunos de los ejemplos de directrices indicadas abajo, algunas de las entradas están registradas como “sin entrada”. Esto se debe a que las directrices están formuladas de manera que las consecuencias adversas en cada uno de los niveles ascendentes, expresadas en una escala de 1 a 10, son ampliamente similares a los seis tipos presentados de C.3.2.2 a C.3.2.7. Sin embargo, en algunos niveles (en la escala de 1 a 10) para algunos de los tipos, se considera que no hay una diferencia suficiente en relación con las entradas de consecuencias inmediatamente inferiores, y esto se registra como “sin entrada”. En forma similar, en los extremos más altos de algunos tipos se considera que no hay consecuencia mayor de la entrada más alta presentada, y por esta razón las entradas del extremo más alto se registran como “sin entrada”. En consecuencia, lógicamente sería incorrecto eliminar las líneas “sin entrada” y compactar la escala).

Entonces, usando el siguiente como un grupo ejemplo de directrices, cuando se consideran las consecuencias adversas de un incidente de seguridad de la información sobre el negocio de una organización, a partir de:

- divulgación no autorizada de información,
- modificación no autorizada de información,
- rechazo (repudio) de información,
- no disponibilidad de información y/o servicio y
- destrucción de información y/o servicio.

El primer paso es considerar cuál de los siguientes tipos es pertinente. Para los que se consideran pertinentes, la directriz del tipo se debería usar para determinar el impacto adverso real sobre las operaciones (o el valor) para entrada al formulario de reporte de incidentes de seguridad de la información.

C.3.2.2 Pérdida financiera/interrupción de las operaciones del negocio

Las consecuencias de la divulgación y la modificación no autorizada, el repudio, al igual que la no disponibilidad y la destrucción de esta información, pueden ser la pérdida financiera, por ejemplo, debido a la reducción el precio de las acciones, fraude o violación de contratos debido a que no se actuó, o no se actuó a tiempo. Igualmente, las consecuencias, particularmente de la no disponibilidad o destrucción de cualquier información, pueden ser interrupciones en las operaciones del negocio. Rectificar y/o recuperarse de estos incidentes requerirá invertir tiempo y esfuerzo. Esto en algunos casos será significativo y se debería considerar. Para usar un

denominador común, el tiempo hasta la recuperación se debería calcular para una unidad de tiempo de personal y convertirla a un costo financiero. Este costo se debería calcular por referencia al costo normal para una persona mes al grado/nivel adecuado dentro de la organización. Se debería usar la siguiente directriz:

1. Da como resultado pérdidas/costos financieros de x 1 o menos

2. Da como resultado pérdidas/costos financieros de entre x_1 +1 y x_2

3. Da como resultado pérdidas/costos financieros de entre x_2 +1 y x_3

4. Da como resultado pérdidas/costos financieros de entre x_3 +1 y x_4

5. Da como resultado pérdidas/costos financieros de entre x_4 +1 y x_5

6. Da como resultado pérdidas/costos financieros de entre x_5 +1 y x_6

7. Da como resultado pérdidas/costos financieros de entre x_6 +1 y x_7

8. Da como resultado pérdidas/costos financieros de entre x_7 +1 y x_8

9. Da como resultado pérdidas/costos financieros de más de x_8

10. La organización saldrá del negocio

En donde, x_i (i = 1, 2, …, 8) representa las pérdidas/costos financieros en ocho grados/niveles que se determinan por la organización en su contexto.

C.3.2.3 Intereses comerciales y económicos

Es necesario proteger la información comercial y la económica, y se le asigna un valor considerando su valor para los competidores o el efecto que su puesta en peligro puede tener en los intereses comerciales. Se debería usar la siguiente directriz:

1. Ser de interés para un competidor, pero no tiene valor comercial.

2. Ser de interés para un competidor, a un valor que es y_1 o menos (volumen de negocios).

3. Ser de un valor para un competidor, a un valor que está entre y_1 + 1 y y_2 (volumen de negocios) y causar pérdida financiera, o pérdida del potencial de obtener ganancias, o facilitar ganancias o ventajas inadecuadas para individuos u organizaciones, o constituir una violación de las promesas adecuadas acerca de mantener la confidencialidad de la información suministrada por terceras partes.

4. Ser de valor para un competidor, a un valor que es y_2 + 1 y y_3 (volumen de negocios).

5. Ser de valor para un competidor, a un valor que está entre y_3 + 1 y y_4 (volumen de negocios)

6. Ser de valor para un competidor, a un valor que es superior a y_4 + 1 (volumen de negocios).

7. Sin entrada[1].

8. Sin entrada.

9. Puede perjudicar sustancialmente los intereses comerciales o perjudicar sustancialmente la viabilidad financiera de la organización.

10. Sin entrada.

En donde, y_i (i = 1, 2, …, 4) representa los valores para un competidor en términos de rotación, en cuatro grados/niveles que determina la organización en su contexto.

C.3.2.4 Información personal

En donde se retiene y procesa información acerca de individuos, es correcto moral y éticamente, y ocasionalmente lo exige la ley, que la información sea protegida contra divulgación no autorizada que en el mejor de los casos puede dar como resultado humillación, y en el peor de los casos una acción legal adversa, por ejemplo, con base en la legislación sobre protección de datos. Igualmente, se requiere que la información acerca de personas sea siempre correcta, ya que una modificación no autorizada que dé como resultado información incorrecta puede tener efectos similares en lo que respecta a divulgación no autorizada. También es importante que la información acerca de personas no deje de estar disponible ni sea destruida, ya que esto puede dar como resultado decisiones equivocadas o que no se tomen acciones en el tiempo requerido, con efectos similares para divulgación o modificación no autorizadas. Se debería usar la siguiente directriz:

1. Malestar menor (preocupación) para un individuo (rabia, frustración, desilusión), pero no ocurre violación de requisitos legales o reglamentarios.

2. Malestar (preocupación) para un individuo (rabia, frustración, desilusión), pero no ocurre violación de requisitos legales o reglamentarios.

3. Violación de un requisito legal, reglamentario o ético, o intención anunciada, sobre la protección de la información, que conduce a humillación menor para un individuo.

4. Violación de un requisito legal, reglamentario o ético, o intención anunciada, sobre la protección de la información, que conduce a humillación significativa para un individuo o una humillación menor a un grupo de individuos.

5. Violación de un requisito legal, reglamentario o ético, o intención anunciada, sobre la protección de la información, que conduce a humillación grave para un individuo.

6. Violación de un requisito legal, reglamentario o ético, o intención anunciada, sobre la protección de la información, que conduce a humillación grave para un grupo de individuos.

7. Sin entrada[1].

8. Sin entrada[1].

9. Sin entrada[1]

[1] El término “sin entrada” significa que no hay una entrada correspondiente para este nivel de impacto.

10. Sin entrada.

C.3.2.5 Obligaciones legales y reglamentarias

Los datos mantenidos y procesados por una organización se pueden someter, mantener y procesar, con el fin de permitir que una organización cumpla sus obligaciones legales y reglamentarias. El incumplimiento de estas obligaciones, ya sea en forma intencional o no, puede dar como resultado que se tomen acciones legales y administrativas contra los individuos dentro de la organización involucrada.

Estas acciones pueden dar como resultado multas y sentencias en prisión. Se debería usar la siguiente directriz:

1. Sin entrada.

2. Sin entrada.

3. Notificación de cumplimiento, demanda civil o delito penal que dan como resultado daños financieros/sanción de z_1 o menos.

4. Notificación de cumplimiento, demanda civil o delito penal que da como resultado daños financieros/ sanción de entre z_1+1 y $z_{2.}$

5. Notificación de cumplimiento, demanda civil o delito penal que dan como resultado daños financieros/ sanción de entre $z_2 + 1$ y z_3 o una condena en prisión de hasta dos años.

6. Notificación de cumplimiento, demanda civil o delito penal que dan como resultado daños financieros/sanciones de entre $z_3 + 1$ y z_4, o una condena en prisión de dos a diez años.

7. Notificación de cumplimiento, demanda civil o delito penal que dan como resultado daños financieros ilimitados/sanciones, o una condena en prisión superior a diez años.

8. Sin entrada.

9. Sin entrada.

10. Sin entrada.

C.3.2.6 Operaciones de gestión y del negocio

La información puede ser de una naturaleza tal, que ponerla en peligro afectaría el desempeño eficaz de la organización. Por ejemplo, la información relacionada con un cambio en una política puede provocar reacción pública si es divulgada, en un grado tal, que no sería posible implementar la política. La modificación, repudio o no disponibilidad de información relacionada con aspectos financieros, o software informático, también pueden tener ramificaciones graves para la operación de la organización. Además, el repudio de obligaciones puede tener consecuencias adversas para el negocio. Se debería usar la siguiente directriz:

1. Operación ineficiente de una parte de la organización.

2. Sin entrada.

3. Afectar la gestión adecuada de la organización y su operación.

4. Sin entrada.

5. Impedir el desarrollo u operación eficaces de las políticas de la organización.

6. Desventaja para la organización en negociaciones comerciales o de políticas con otros.

7. Impedir en forma grave el desarrollo u operación de las principales políticas organizacionales, o apagar o interrumpir sustancialmente de cualquier otra manera operaciones significativas.

8. Sin entrada.

9. Sin entrada.

10. Sin entrada.

C.3.2.7 Pérdida del buen nombre

La divulgación, modificación, repudio o no disponibilidad de información no autorizados puede conducir a una pérdida del buen nombre de la organización, lo que da como resultado daño a su reputación, pérdida de credibilidad y otras consecuencias adversas. Se debería usar la siguiente directriz:

1. Sin entrada.

2. Causa humillación dentro de la organización.

3. Afecta adversamente las relaciones con accionistas, clientes, proveedores, empleados, usuarios de terceras partes, organismos de reglamentación, gobierno, otras organizaciones o el público, lo que genera publicidad adversa local/regional.

4. Sin entrada.

5. Afecta adversamente las relaciones con accionistas, clientes, proveedores, empleados, usuarios de terceras partes, organismos de reglamentación, gobierno, otras organizaciones o el público, lo que genera publicidad adversa nacional.

6. Sin entrada.

7. Afecta considerablemente las relaciones con accionistas, clientes, proveedores, empleados, usuarios de terceras partes, organismos de reglamentación, gobierno, otras organizaciones o el público, lo que genera publicidad adversa generalizada.

8. Sin entrada.

9. Sin entrada.

10. Sin entrada.

ANEXO D
(Informativo)

REPORTES Y FORMULARIOS DE EVENTOS, INCIDENTES Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

D.1 INTRODUCCIÓN

Este anexo contiene ejemplos de los elementos que se registran para eventos, incidentes y vulnerabilidades de seguridad de la información, y ejemplos de formularios para reportar eventos, incidentes y vulnerabilidades de seguridad de la información, con las notas relacionadas. Se hace énfasis en que son ejemplos. Existen otros, como los que presenta la norma sobre “Formularios para descripción e intercambio de objetos de incidentes (IODEF)”.

D.2 EJEMPLOS DE ELEMENTOS EN LOS REGISTROS

D.2.1 Ejemplos de elementos del registro de eventos de seguridad de la información

Incluye información básica del evento de seguridad de la información, como por ejemplo cuándo, qué, cómo y por qué ocurrió el evento, al igual que la información de contacto de la persona que reporta.

Información básica

Fecha del evento

Número del evento

Evento relacionado y/o número de incidentes (si es aplicable)

Detalles de la persona que reporta

Nombre

Información de contacto, tal como dirección, organización, departamento, teléfono y correo electrónico

Descripción del evento

Qué ocurrió

Cómo ocurrió

Por qué ocurrió

Consideraciones iniciales sobre componentes/activos afectados

Impactos adversos para el negocio

Cualquier vulnerabilidad identificada

Detalles del evento

Fecha y hora en la que ocurrió el evento

Fecha y hora en la que se descubrió el evento

Fecha y hora en la que se reportó el evento

D.2.2 Ejemplos de elementos del registro de incidentes de seguridad de la información

Incluye información básica del incidente de seguridad de la información, como por ejemplo cuándo, qué, cómo y por qué ocurrió el incidente, al igual que la categoría e impacto del incidente y el resultado de la respuesta al incidente.

Información básica

Fecha del incidente

Número del incidente

Evento relacionado y/o número de incidentes (si es aplicable)

Persona que reporta

Nombre

Información de contacto, tal como dirección, organización, departamento, teléfono y correo electrónico

Miembro del punto de contacto (PC)

Nombre

Información de contacto, tal como dirección, organización, departamento, teléfono y correo electrónico

Detalles del miembro de ISIRT

Nombre

Información de contacto, tal como dirección, organización, departamento, teléfono y correo electrónico

Descripción del incidente

Qué ocurrió

Cómo ocurrió

Por qué ocurrió

Consideraciones iniciales sobre componentes/activos afectados

Impactos adversos para el negocio

Cualquier vulnerabilidad identificada

Detalles del incidente

Fecha y hora en la que ocurrió el incidente

Fecha y hora en la que se descubrió el incidente

Fecha y hora en la que se reportó el incidente

Categoría del incidente

Componentes/activos afectados

Impacto adverso para el negocio/efecto del incidente

Costo total de recuperación del incidente

Resolución del incidente

Persona(s)/autor(es) involucrados (si el incidente fue causado por personas).

Descripción del autor

Motivación real/percibida

Acciones tomadas para resolver el incidente.

Acciones planeadas para resolver el incidente

Acciones pendientes

Conclusión

Individuos internos/entidades notificadas

Individuos internos/entidades notificadas

D.2.3 Ejemplos de elementos del registro de vulnerabilidades de seguridad de la información

Incluye información básica de la vulnerabilidad de seguridad de la información, como por ejemplo cuándo, qué, cómo se identificó la vulnerabilidad, al igual que su impacto potencial y su resolución.

Información básica

Fecha de la vulnerabilidad identificada

Número de la vulnerabilidad

Detalles de la persona que reporta

Nombre

Información de contacto, tal como dirección, organización, departamento, teléfono y correo electrónico

Descripción de la vulnerabilidad

Resolución de la vulnerabilidad

D.3 CÓMO USAR LOS FORMULARIOS

D.3.1 Formato de fecha y hora

Las fechas se deberían registrar en el formato CCYY-MM-DD (y si se requiere, HH-MM-SS). Si es pertinente, se debería usar el TUC (Tiempo Universal Coordinado), de manera que se facilite la comparación cuando muchos eventos pueden estar ocurriendo a través de zonas horarias (y al menos indicar la compensación de la UTC aplicada a la hora).

D.3.2 Notas acerca de la información de los formularios

El propósito de los formularios de reporte de eventos e incidentes de seguridad de la información es proporcionar información acerca de un evento de seguridad de la información, y entonces, si se determina que es un incidente de seguridad de la información, informar a las personas adecuadas acerca de dicho evento.

Si sospecha que está en progreso un evento de seguridad de la información, o puede haber ocurrido, particularmente uno que puede causar pérdida sustancial o daño a la propiedad o a la reputación de la organización, usted debería completar *inmediatamente* el formulario de reporte de eventos de seguridad de la información (véase la primera parte de este anexo), de acuerdo con los procedimientos especificados en el esquema de gestión de incidentes de seguridad de la información, de la organización.

La información que usted suministre se usará para iniciar la evaluación adecuada, la cual determinará si el evento se ha de clasificar o no como un incidente de seguridad de la información, y si es necesaria una medida correctiva para prevenir o limitar cualquier pérdida o daño. Dada la naturaleza de este proceso, potencialmente crítica en el tiempo, *no es esencial llenar en este momento todos los campos del formulario de reporte.*

Si usted es el miembro del PoC (Punto de Contacto) que examina los formularios llenos parcial o totalmente, entonces deberá decidir si el evento se debe clasificar como un incidente de seguridad de la información. Si el evento se clasifica así, llene el formulario con la mayor cantidad posible de información que pueda, y envíe al ISIRT los formularios tanto de evento como de incidente. Ya sea que el evento de seguridad de la información se clasifique o no como incidente, la base de datos de eventos/incidentes/vulnerabilidades se debería actualizar.

Si usted es el miembro del ISIRT que examina los formularios de eventos e incidentes de seguridad de la información enviados a un miembro del PC, entonces el formulario de incidentes se debería actualizar a medida que avanza la investigación y se debería actualizar la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

El propósito del formulario de reporte de vulnerabilidades del sistema de información es brindar información acerca de una vulnerabilidad percibida y actuar como el depósito de información acerca de la resolución de la vulnerabilidad reportada.

Por favor, tenga en cuenta las siguientes directrices al completar los formularios:

- Se recomienda llenar y enviar el formulario por un medio electrónico[2]. (Cuando existan problemas con los mecanismos de reporte electrónico (por ejemplo, correo electrónico) o se considere que existen, incluyendo cuando es posible que el sistema sea objeto de ataque y los formularios de reporte electrónicos puedan ser leídos por personas no autorizadas, se debería utilizar un medio de reporte alternativo. Los medios alternativos pueden ser: en persona, por teléfono o por medio de mensajes de texto).

- Suministre sólo información basada en hechos, no especule para completar los campos. En donde sea necesario suministrar información que no puede confirmar, por favor, indique claramente que la información no es confirmada, y qué le hace pensar a usted que es verdadera.

- Es conveniente que suministre sus detalles de contacto completos. Puede ser necesario contactarle a usted, ya sea con urgencia o en una fecha posterior, para obtener información adicional concerniente a su reporte.

Si posteriormente descubre que la información que ha proporcionado es inexacta, incompleta o engañosa, es conveniente que la corrija y que reenvíe el formulario.

[2] Por ejemplo, en un formulario de página web segura con un enlace a la base de datos de datos electrónica de eventos/incidentes/vulnerabilidades de seguridad de la información. En el mundo de hoy, la operación de un esquema que utiliza papel sería muy dispendiosa. Sin embargo, también es necesario contar con este esquema, para cuando no sea posible usar un esquema electrónico.

D.4 EJEMPLO DE FORMULARIOS

D.4.1 Ejemplo de formulario para el reporte de eventos de seguridad de la información

Reporte de evento de seguridad de la información

1. Fecha del evento	**Página 1 de 1**	
2. Número del evento[3]	**3. (Si es aplicable) Número de identificación de eventos y/o incidentes relacionados**	
4. DETALLES DE LA PERSONA QUE REPORTA		
4.1 Nombre	**4.2 Dirección**	
4.3 Organización	**4.4 Departamento**	
4.5 Teléfono	**4.6 Correo electrónico**	
5. DESCRIPCIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN		
5.1 Descripción del evento: • Qué ocurrió • Cómo ocurrió • Por qué ocurrió • Consideraciones iniciales sobre componentes/activos afectados • Impactos adversos para el negocio • Cualquier vulnerabilidad identificada		
6. DETALLES DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN		
6.1 Fecha y hora en la que ocurrió el evento		
6.2 Fecha y hora en la que se descubrió el evento		
6.3 Fecha y hora en la que se reportó el evento		
6.4 ¿La respuesta a este evento ya ha finalizado? ***(Marque la respuesta adecuada).***	**SÍ**	**NO**
6.5 En caso afirmativo, especifique cuánto duró el evento en días/horas/minutos		

[3] Los números de los eventos los debería asignar el líder del ISIRT de la organización.

D.4.2 Ejemplo de formulario para el reporte de incidentes de seguridad de la información

Reporte de incidente de seguridad de la información

1. Fecha del incidente	**Página 1 de 6**	
2. Número del incidente[4]	**3. (Si es aplicable) Números de identificación de eventos y/o incidentes relacionados**	
4. DETALLES DEL MIEMBRO DEL PUNTO DE CONTACTO (PC)		
4.1 Nombre	**4.2 Dirección**	
4.3 Organización	**4.4 Departamento**	
4.5 Teléfono	**4.6 Correo electrónico**	
5. DETALLES DEL MIEMBRO DE ISIRT		
5.1 Nombre	**5.2 Dirección**	
5.3 Organización	**5.4 Departamento**	
5.5 Teléfono	**5.6 Correo electrónico**	
6. DESCRIPCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
6.1 Descripción adicional del incidente: Qué ocurrió Cómo ocurrió Por qué ocurrió Consideraciones iniciales sobre componentes/activos afectados Impactos adversos para el negocio Cualquier vulnerabilidad identificada		
7. DETALLES DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
7.1 Fecha y hora en la que ocurrió el incidente		
7.2 Fecha y hora en la que se descubrió el incidente		
7.3 Fecha y hora en la que se reportó el incidente		
7.4 Identificación/detalles de contacto de la persona que hace el reporte		
7.5 ¿Ya finalizó el incidente? ***(Marque la respuesta adecuada).***	**SÍ**	**NO**
7.6 En caso afirmativo, especifique cuánto duró el incidente en días/horas/minutos		

[4] Los números de los incidentes los debería asignar el líder del ISIRT de la organización y se deberían vincular a los números de los eventos asociados.

Reporte de incidente de seguridad de la información

Página 2 de 6		
8. CATEGORÍA DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
(Marque una de las siguientes opciones, y a continuación complete la sección relacionada más abajo)	**8.1 Real** ***(incidente que ocurrió)***	**8.2 Sospechado** ***(se sospecha que ha ocurrido, pero no se ha confirmado)***
***(uno de)* 8.3 Desastre natural**	*__ (Indique los tipos de amenazas involucradas)*	
Terremoto __ Volcán __ Inundación __ Viento muy fuerte __ **Descarga electromagnética __ Tsunami __ Derrumbe __ Otros __**		
Especifique:		
***(uno de)* 8.4 Conflicto social** *__ (Indique los tipos de amenazas involucradas)* **Bedin (disturbio)___ Ataque terrorista __ Guerra __** **Otros __**		
Especifique:		
***(uno de)* 8.5 Daño físico** *__ (Indique los tipos de amenazas involucradas)*		
Incendio __ Agua __ **Electrostática __** **Ambiente nefasto (contaminación, polvo, corrosión, congelamiento) __** **Destrucción de equipos __ Destrucción de medios __ Robo de equipos __** **Robo de medios __ Pérdida de equipos __ Pérdida de medios __** **Alteración de equipos __ Alteración de medios __ Otros __**		
Especifique:		
***(uno de)* 8.6 Fallas en la infraestructura** *__ (Indique los tipos de amenazas involucradas)*		
Fallas en la alimentación eléctrica __ Fallas en las redes __ **Fallas en el aire acondicionado __** **Fallas en el suministro de agua __ Otros __**		
Especifique:		
***(uno de)* 8.7 Perturbación por radiación** *__ (Indique los tipos de amenazas involucradas)*		
Radiación electromagnética __ Pulsos electromagnéticos __ **Interferencia electrónica __ Fluctuación de tensión __ Radiación térmica __ Otros __**		
Especifique:		
***(uno de)* 8.8 Falla técnica**		
Falla en el hardware __ Mal funcionamiento del software __ **Sobrecarga (saturación de la capacidad de los sistemas de información) __** **Violación de la mantenibilidad*__ Otros __**		
Especifique:		

Reporte de incidente de seguridad de la información

Página 3 de 6
8. CATEGORÍA DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN
(uno de)* 8.9 *Malware __ *(Indique los tipos de amenazas involucradas)*
Gusano de red __ Troyano __ *Botnet* __ Ataques combinados __ **Página web con código malicioso incrustado __ Sitio de alojamiento con código malicioso__ Otros __**
Especifique:
***(uno de)* 8.10 Ataque técnico** *(Indique los tipos de amenazas involucradas)*
Escaneo de redes __ Aprovechamiento de vulnerabilidades __ Aprovechamiento de puertas traseras __ **Intentos de acceso __ interferencia __ Denegación del servicio __ Otros __**
Especifique:
***(uno de)* 8.11 Violación de reglas** __ *(Indique los tipos de amenazas involucradas)*
Uso no autorizado de recursos __ Violación de los derechos de autor __ Otros __
Especifique:
***(uno de) 8.12* Puesta en peligro de las funciones** *(Indique los tipos de amenazas involucradas)*
Abuso de derechos __ Falsificación de derechos, denegación de acciones __ Operaciones incorrectas __ **Violación de la disponibilidad de personal __ Otros __**
Especifique:
***(uno de)* 8.13 Puesta en peligro de la información** __ *(Indique los tipos de amenazas involucradas)*
Interceptación __ Espionaje __ "Chuzada" de teléfonos __ Divulgación __ **Enmascaramiento __ Ingeniería social __ *Phishing* de redes __ Robo de datos __** **Pérdida de datos __ Alteración de datos __ Error en los datos __ Análisis de flujo de datos __** **Detección de posición __ Otros __**
Especifique:
***(uno de)* 8.14 Contenidos peligrosos** *(Indique los tipos de amenazas involucradas)*
Contenido ilegal __ Contenido que provoca pánico __ Contenido malicioso __ **Contenido abusivo __ Otros __**
-Especifique:
8.15 Otros ___ *(Si no se ha determinado que el incidente pertenezca a la categoría anterior, marque aquí)*
Especifique:

Reporte de incidente de seguridad de la información

Página 4 de 6			
9. Componentes/activos afectados[5]			
Componentes/activos afectados *(si los hay)*	*(Suministre descripciones de los componentes/activos afectados por el incidente o relacionados con él, incluidos los números de serie, licencia y versión, en donde sea pertinente.)*		
9.1 Información/Datos			
9.2 Hardware			
9.3 Software			
9.4 Comunicaciones			
9.5 Documentación			
9.6 Procesos			
9.7 Otros			
10. IMPACTO ADVERSO PARA EL NEGOCIO/EFECTO DEL INCIDENTE *Para cada uno de los siguientes, indique en la casilla si es pertinente, y luego en la columna "valor" registre el(los) nivel(es) de impacto adverso sobre el negocio, que comprendan todas las partes afectadas por el incidente, en una escala de 1 a 10, usando la directriz para las categorías de: pérdida financiera/Interrupción de las operaciones del negocio, intereses comerciales y económicos, información personal, obligaciones legales y reglamentarias, operaciones de gestión y del negocio, y pérdida del buen nombre. (Véanse los ejemplos en el Anexo C.3.2). Registre en la columna "directriz" las letras código para las directrices aplicables, y si se conocen los costos reales, regístrelos en la columna "Costo"*			
VALOR	**DIRECTRIZ**	**COSTO**	
10.1 Violación de la confidencialidad ___ ***(es decir, divulgación no autorizada)***			
10.2 Violación de la integridad ___ ***(es decir, modificación no autorizada)***			
10.3 Violación de la disponibilidad ___ ***(es decir, no disponibilidad)***			
10.4 Violación del no repudio ___			
10.5 Destrucción ___			
11. COSTOS TOTALES DE RECUPERACIÓN DEL INCIDENTE			
(Cuando sea posible, se debe presentar el costo total real de la recuperación del incidente como un todo, en la columna de "valor" usando una escala de 1 a 10 y debajo de "costo" en valor real.	**VALOR**	**DIRECTRIZ**	**COSTO**

[5] Esto es para más detalles de los componentes/activos afectados, y está disponible como procedimientos de investigación y análisis (en las etapas tempranas del análisis de eventos e incidentes normalmente sólo se recolectará información de "alto nivel").

Reporte de incidente de seguridad de la información

12. RESOLUCIÓN DEL INCIDENTE
Página 5 de 6
12.1 Fecha de inicio de la investigación del incidente
12.2 Nombre(s) del(los) investigador(es) del incidente
12.3 Fecha de finalización del incidente
12.4 Fecha de finalización del impacto
12.5 Fecha de finalización de la investigación del incidente
12.6 Referencia y ubicación del reporte de la investigación
13. (SI EL INCIDENTE FUE CAUSADO POR PERSONAS) (PERSONA(S)/AUTOR(ES)INVOLUCRADOS)
(uno de) Persona __ Organización/institución establecida legalmente ___ Grupo organizado __ Accidente __ No hay autor __ *Por ejemplo, elementos naturales, falla de los equipos, error humano*
14. DESCRIPCIÓN DEL AUTOR
15. MOTIVACIÓN REAL O PERCIBIDA
(uno de) Ganancia criminal financiera __ Pasatiempo/piratería informática __ Política/terrorismo __ Venganza __ Otros __
Especifique:
16. ACCIONES <u>TOMADAS</u> PARA RESOLVER EL INCIDENTE *(Por ejemplo, "ninguna acción", "acción interna", investigación "externa" por...)*
17. ACCIONES <u>PLANIFICADAS</u> PARA RESOLVER EL INCIDENTE *(Por ejemplo, véanse los ejemplos anteriores)*
18. ACCIONES PENDIENTES *(por ejemplo, otro personal aún necesita la investigación*

Reporte de incidente de seguridad de la información

Página 6 de 6		
19. CONCLUSIÓN		
(marque mayor o menor según sea pertinente, e incluya una breve descripción para justificar la conclusión) **Mayor ___ Menor ___** *(Indique cualquier otra conclusión)*		
20. INDIVIDUOS INTERNOS/ENTIDADES NOTIFICADAS		
(Estos detalles los debe completar la persona pertinente con responsabilidades de seguridad de la información, y debe establecer las acciones requeridas). Según sea pertinente, esto lo puede ajustar el jefe de seguridad de información de la organización, u otro funcionario responsable)	**Líder/funcionario responsable de seguridad de la información __**	**Líder del ISIRT __**
	Gerente del sitio __ *(indique qué sitio)*	**Líder de sistemas de información __**
	Originador del reporte __	**Líder del originador del reporte/** **Gerencia afectada del usuario de la línea***
Otros *(por ejemplo, mesa de ayuda, recursos humanos, gerencia, auditoría interna,*		
Especifique:		
21. INDIVIDUOS EXTERNOS/ENTIDADES NOTIFICADAS		
(Estos detalles los debe completar la persona pertinente con responsabilidades de seguridad de la información, y debe establecer las acciones requeridas). Según sea pertinente, esto lo puede ajustar el jefe de seguridad de información de la organización, u otro funcionario responsable)	**Policía**	**Otros** *(por ejemplo, organismos de reglamentación, ISIRT externos*
Especifique:		
21. FIRMAS		
ORIGINADOR	**Revisor**	**Revisor**
Firma digital	**Firma digital**	**Firma digital**
Nombre	**Nombre**	**Nombre**
Rol	**Rol**	**Rol**
Fecha	**Fecha**	**Fecha**

D.4.3 Ejemplo de formulario para el reporte de vulnerabilidades de seguridad de la información

Reporte de vulnerabilidad de seguridad de la información

1. Fecha de identificación de la vulnerabilidad	**Página 1 de 1**		
2. Número de la vulnerabilidad[6]			
3. DETALLES DE LA PERSONA QUE REPORTA			
3.1 Nombre	**3.2 Dirección**		
3.3 Organización	**3.4 Departamento**		
3.5 Teléfono	**3.6 Correo electrónico**		
4. DESCRIPCIÓN DE LA VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN			
4.1 Fecha y hora en la que se reportó la vulnerabilidad			
4.2 Descripción narrada de la vulnerabilidad de seguridad de la información percibida: • Cómo se detectó la vulnerabilidad • Características de la vulnerabilidad: física, técnica, etc. • Si es técnica, qué activos, componentes de redes/TI fueron involucrados • Componentes/Activos que podrían afectarse si se aprovechara esa vulnerabilidad • Impactos adversos potenciales en el negocio si se aprovechara esa vulnerabilidad			
5. RESOLUCIÓN DE LA VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN			
5.1 ¿Se confirmó la vulnerabilidad? *(Marque la respuesta adecuada).*		**SÍ**	**NO**
5.2 Fecha y hora en que se confirmó la vulnerabilidad			
5.3 Nombre de la persona que autoriza	**5.4 Dirección**		
5.5 Organización			
5.6 Teléfono	**5.7 Correo electrónico**		
5.8 ¿Se solucionó la vulnerabilidad? *(Marque la respuesta adecuada).*		**SÍ**	**NO**
5.9 Descripción narrada de cómo se solucionó la vulnerabilidad de seguridad de la información, con la fecha y hora y el nombre de la persona que autoriza la resolución.			

[6] Los números de las vulnerabilidades los debería asignar el líder del ISIRT de la organización.

ANEXO E
(Informativo)

ASPECTOS LEGALES Y REGLAMENTARIOS

Los siguientes aspectos legales y reglamentarios de la gestión de incidentes de seguridad de la información se deberían tener en cuenta en la política de gestión de incidentes de seguridad de la información y esquemas asociados:

- **Se brinda protección adecuada de datos y privacidad de la información personal.** En los países en los que existe legislación específica acerca de confidencialidad e integridad de los datos, con frecuencia está limitada al control de datos personales. Puesto que los incidentes de seguridad de la información necesitan ser atribuidos habitualmente a un individuo, en consecuencia es posible que sea necesario registrar y gestionar la información de naturaleza personal, de acuerdo con esto. Por tanto, un enfoque estructurado para la gestión de incidentes de seguridad de la información debe tener en cuenta la protección adecuada de la privacidad. Esto incluye:

  - aquellos individuos con acceso a datos personales no deberían, en la medida en que resulte práctico, conocer en persona a los investigados.

  - es conveniente que los individuos que tengan acceso a datos personales firmen acuerdos de no divulgación, antes de que se les permita el acceso a ellos.

  - la información sólo se debería usar con el propósito expreso para el cual se ha obtenido, es decir, para la investigación de incidentes de seguridad de la información.

- **Se mantienen los registros adecuados.** Algunas leyes nacionales exigen que las compañías lleven registros adecuados de sus actividades para revisión en el proceso de auditoría anual de la organización. Existen requisitos similares en relación con organizaciones gubernamentales. En algunos países se exige que las organizaciones reporten o generen archivos acerca del cumplimiento de la ley (por ejemplo, acerca de cualquier caso que pueda involucrar un delito grave o penetración en un sistema gubernamental confidencial).

- **Hay controles implementados para asegurar el cumplimiento de obligaciones comerciales contractuales.** En donde hay requisitos vinculantes acerca de la prestación de un servicio de gestión de incidentes de seguridad de la información, por ejemplo, los tiempos de respuesta requeridos, la organización se debería asegurar de que se suministre la seguridad de información adecuada, para asegurar que todas las obligaciones se puedan cumplir en todas las circunstancias. (En relación con esto, si una organización contrata soporte con una parte externa, por ejemplo, una ISIRT externa, entonces se debería asegurar de que todos los requisitos, incluidos los tiempos de respuesta, estén incluidos en el contrato con la parte externa).

- **Se abordan los aspectos legales relacionados con políticas y procedimientos.** Las políticas y procedimientos asociados con el esquema de gestión de incidentes de seguridad de la información se deberían revisar en relación con problemas legales y reglamentarios potenciales, por ejemplo, si hay declaraciones acerca de acciones disciplinarias y/o legales contra quienes causen incidentes de seguridad de la información. En algunos países no es fácil dar por terminado un contrato laboral.

- **Las renuncias a responsabilidad se examinan para determinar su validez legal.** Todas las renuncias a responsabilidad acerca de acciones tomadas por el equipo de gestión de incidentes de información, y cualquier personal externo de soporte, se deberían examinar para determinar su validez.

- **Los contractos con personal externo de apoyo cubren todos los aspectos requeridos.** Los contratos con cualquier personal externo de soporte, por ejemplo, de un ISIRT externo, se deberían examinar concienzudamente en relación con las renuncias de responsabilidad civil, no divulgación, y las implicaciones de una asesoría incorrecta.

- **Los acuerdos de no divulgación son ejecutables.** Es posible solicitar a los miembros del equipo de gestión de incidentes de seguridad de la información que firmen acuerdos de no divulgación, tanto al iniciar, como al finalizar el contrato. En algunos países, es posible que la firma de acuerdos de no divulgación no sea ejecutable legalmente; es conveniente examinar esto.

- **Se tienen en cuenta requisitos sobre cumplimiento de la ley.** Es necesario aclarar los temas asociados con la posibilidad de que los organismos encargados de velar por el cumplimiento de la ley pudieran solicitar legalmente información de un esquema de gestión de incidentes de seguridad de la información. Es posible que se requiera claridad sobre el nivel mínimo exigido por la ley al cual se deberían documentar los eventos, y el tiempo que se debería retener la documentación.

- **Los aspectos sobre responsabilidad civil son claros.** Es necesario aclarar los temas sobre responsabilidad civil potencial y los controles requeridos relacionados que se deben implementar. Algunos ejemplos de eventos que pueden tener en cuenta aspectos de responsabilidad civil asociados son:

  - si un incidente puede afectar a otra organización (por ejemplo, al divulgar información compartida), no se notifica oportunamente y la otra organización sufre un impacto adverso,

  - si se descubre una nueva vulnerabilidad en un producto, no se notifica al distribuidor y tiempo después ocurren incidentes mayores relacionados con dicho impacto, en una o varias organizaciones,

  - no se hace un reporte en el que, en el país particular, se exige que las organizaciones reporten o generen archivos para las organizaciones que velan por el cumplimiento de la ley, acerca de cualquier caso que pueda involucrar un delito grave o penetración en un sistema gubernamental confidencial, o parte de la infraestructura nacional crítica,

  - se divulga información que parece indicar que alguien, o una organización, puede estar involucrado en un ataque. Esto puede afectar la reputación y el negocio de la persona u organización implicada,

  - se divulga información de que puede haber un problema con un elemento particular de software, y se descubre que esto no es cierto.

- **Se tienen en cuenta requisitos reglamentarios específicos.** En donde así lo exigen los requisitos reglamentarios específicos, los incidentes se deberían reportar a un organismo designado, por ejemplo, como se exige en la industria de energía nuclear, las compañías de telecomunicaciones y los proveedores de servicios de Internet.

- **Las acciones judiciales o procedimientos disciplinarios internos pueden ser exitosos.** Deberían haber implementados controles de seguridad de la información adecuados, que incluyan rastros de auditoría a prueba de alteración que se pueda comprobar, para poder emprender acciones judiciales, o entablar procedimientos disciplinarios internos contra los “atacantes”, ya sea que el ataque sea técnico o físico.

  Como apoyo de esto, habitualmente se requerirá recoger evidencia que sea admisible para las cortes nacionales adecuadas u otro foro disciplinario. Debería ser posible demostrar que:

  - los registros están completos y no se han alterado de ninguna manera,
  - las copias de evidencia electrónica son idénticas a los originales y esto se puede comprobar y
  - cualquier sistema de TI del cual se haya recolectado evidencia estaba operando correctamente en el momento de registro de la evidencia.

- **Se tienen en cuenta los aspectos legales asociados con técnicas de seguimiento.** Las implicaciones del uso de técnicas de seguimiento deben tenerse en cuenta en el contexto de la legislación nacional pertinente. El carácter legal de diferentes técnicas variará de un país a otro. Por ejemplo, en algunos países es necesario hacer conocer a las personas que se lleva a cabo el seguimiento de actividades, incluidas técnicas de vigilancia. Los factores que es necesario considerar incluyen quién/qué se monitorea, cómo se lleva a cabo el seguimiento y cuándo ocurre. También es conveniente tener en cuenta que el seguimiento/vigilancia en el contexto de IDS se trata específicamente en la norma ISO/IEC 18043.

- **La política de uso aceptable se define y comunica.** Es conveniente definir, documentar y comunicar a todos los usuarios previstos las prácticas/uso aceptables dentro de la organización. (Por ejemplo, cuando los usuarios se vinculan a la organización o se les concede acceso a sistemas de información, se les debería informar acerca de la política de uso aceptable, y solicitarles confirmación escrita de que comprenden y aceptan dicha política).

BIBLIOGRAFÍA

ISO/IEC 18043, *Information Technology. Security Techniques. Selection, Deployment and Operations of Intrusion Detection Systems.*

ISO/IEC 20000 (*All Parts*), *Information Technology. Service Management.*

ISO/PAS 22399, *Societal Security. Guidelines for Incident Preparedness and Operational Continuity Management.*

ISO/IEC 27001, *Information Technology. Security Techniques. Information Security Management Systems. Requirements.*

ISO/IEC 27002, *Information Technology. Security Techniques. Code of Practice for Information Security Management.*

ISO/IEC 27003, *Information Technology. Security Techniques. Information Security Management System Implementation Guidance.*

ISO/IEC 27004, *Information Technology. Security Techniques. Information Security Management. Measurement.*

ISO/IEC 27005, *Information Technology. Security Techniques. Information Security Risk Management.*

ISO/IEC 27031, *Information Technology. Security Techniques. Guidelines for Information and Communication Technology Readiness for Business Continuity.*

ISO/IEC 27033-1, *Information Technology. Security Techniques. Network Security. Part 1: Overview and Concepts*

ISO/IEC 27033-2, *Information Technology. Security Techniques. Network Security. Part 2: Guidelines for the Design and Implementation of Network Security*.

ISO/IEC 27033-3, *Information Technology. Security Techniques. Network Security. Part 3: Reference Networking Scenarios. Threats, Design Techniques and Control Issues.*

Internet Engineering Task Force (IETF) Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt?number=2196

Internet Engineering Task Force (IETF) RFC 2350, E*xpectations for Computer Security Incident* Response, http://www.ietf.org/rfc/rfc2350.txt?number=2350

NIST Special Publication 800-61, *Computer Security Incident Handling Guide* (2004), http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

TERENA's *Incident Object Description Exchange Format Data Model and XML Implementation* (IODEF) (Produced by IETF), RFC 5070

Internet Engineering Task Force (IETF) RFC 3227, *Guidelines for Evidence Collection and Archiving*

CESG GOVCERTUK, Incident Response Guidelines (2008), http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information Technology. Security Techniques. Information Security Incident Management.* Geneve. ISO, 2011, 78 p. (ISO IEC 27035).