Norma Española

UNE-EN ISO/IEC 27002

Mayo 2017

Tecnología de la Información

Técnicas de seguridad

Código de prácticas para los controles de seguridad de la información

(ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)

Esta norma ha sido elaborada por el comité técnico CTN 71 *Tecnología de la información*.

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

UNE-EN ISO/IEC 27002

Tecnología de la Información
Técnicas de seguridad
Código de prácticas para los controles de seguridad de la información
(ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)

Information technology. Security techniques. Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015).

Technologies de l'information. Techniques de sécurité. Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015).

Esta norma es la versión oficial, en español, de la Norma Europea EN ISO/IEC 27002:2017, que a su vez adopta las Normas Internacionales ISO/IEC 27002:2013, ISO/IEC 27002:2013/Cor.1:2014 e ISO/IEC 27002:2013/Cor.2:2015.

Esta norma anula y sustituye a las Normas UNE-ISO/IEC 27002:2009 y UNE-ISO/IEC 27002:2015.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org
Depósito legal: M 15630:2017

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO IEC 27002

Febrero 2017

ICS 03.100.70; 35.030

Versión en español

Tecnología de la Información
Técnicas de seguridad
Código de prácticas para los controles de seguridad de la información
(ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)

Information technology. Security techniques. Code of practice for information security controls. (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information. Techniques de sécurité. Code de bonne pratique pour le management de la sécurité de l'information. (ISO/IEC 27002:2013 y compris Cor 1:2014 et Cor 2:2015)

Informationstechnik. Sicherheitsverfahren. Leitfaden für Informationssicherheitsmaßnahmen. (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Esta norma europea ha sido aprobada por CEN/CENELEC el 2017-01-26.

Los miembros de CEN/CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional. Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales pueden obtenerse en la Secretaría Central de CENELEC o en el Centro de Gestión de CEN, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CEN/CENELEC en su idioma nacional, y notificada a la Secretaría Central de CENELEC o al Centro de Gestión de CEN, tiene el mismo rango que aquéllas.

Los miembros de CEN/CENELEC son los organismos nacionales de normalización y los comités electrotécnicos nacionales de los países siguientes: Alemania, Antigua República Yugoslava de Macedonia, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Serbia, Suecia, Suiza y Turquía.

CENTRO DE GESTIÓN DE CEN
Avenue Marnix 17, B-1000 Brussels

SECRETARÍA CENTRAL DE CENELEC
Avenue Marnix 17, B-1000 Brussels

Índice

Prólogo europeo

El texto de la Norma ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015 ha sido elaborado por el Comité Técnico ISO/IEC JTC 1 *Tecnología de la Información* de la Organización Internacional de Normalización (ISO) y de la Comisión Electrotécnica Internacional (IEC) y ha sido adoptada como EN ISO/IEC 27002:2017.

Esta norma europea debe recibir el rango de norma nacional mediante la publicación de un texto idéntico a ella o mediante ratificación antes de finales de agosto de 2017, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de agosto de 2017.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN y/o CENELEC no es(son) responsable(s) de la identificación de dichos derechos de patente.

De acuerdo con el Reglamento Interior de CEN/CENELEC, están obligados a adoptar esta norma europea los organismos de normalización de los siguientes países: Alemania, Antigua República Yugoslava de Macedonia, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Serbia, Suecia, Suiza y Turquía.

Declaración

El texto de la Norma ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015 ha sido aprobado por CEN como Norma EN ISO/IEC 27002:2017 sin ninguna modificación.

Prólogo

ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de tecnologías de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado 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 Norma ISO/IEC 27002 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1 *Tecnología de la Información,* Subcomité SC 27 *Técnicas de seguridad*.

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 la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

Esta segunda edición anula y sustituye a la primera edición (ISO/IEC 27002:2005) que ha sido revisada técnicamente.

0 Introducción

0.1 Antecedentes y contexto

Esta norma internacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001[10] o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de la seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta su(s) entorno(s) específico(s) de riesgo de seguridad de la información.

Organizaciones de todo tipo y tamaño (incluyendo sector público y privado, comercial y sin ánimo de lucro) recogen, procesan, almacenan y transmiten información de muchas formas incluyendo medios electrónicos, físicos y verbales (por ejemplo conversaciones y presentaciones).

El valor de la información trasciende las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, ideas y marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y sus procesos relacionados, los sistemas, las redes y el personal implicados en su operación, manejo y protección son activos que, al igual que otros activos importantes del negocio, resultan valiosos para el negocio de una organización y, en consecuencia, merecen o requieren protección contra diversos peligros.

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocio u otros cambios externos (por ejemplo, nuevas leyes y regulaciones) pueden crear nuevos riesgos relativos a la seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información están siempre presentes. Una seguridad de la información eficaz reduce estos riesgos protegiendo a la organización frente a las amenazas y vulnerabilidades, y en consecuencia reduce el impacto en sus activos.

La seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles se deberían establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización. Un SGSI como el que se especifica en la Norma ISO/IEC 27001[10] constituye una visión holística y coordinada de los riesgos de seguridad de la información de la organización con el fin de implantar un conjunto completo de controles de seguridad de la información en el marco global de un sistema de gestión coherente.

Muchos sistemas de información no han sido diseñados para ser seguros en el sentido de la Norma ISO/IEC 27001[10] y de esta norma. La seguridad que se puede lograr a través de medios técnicos es limitada y debería ser apoyada por una gestión y unos procedimientos apropiados. La identificación de los controles que deberían implantarse requiere una planificación cuidadosa y una atención al detalle. Un buen SGSI necesita el apoyo de todos los empleados de la organización. También puede requerir la participación de las partes interesadas, proveedores, u otras partes externas. Puede ser también necesaria una asesoría especializada por parte de organizaciones 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 asegurados y protegidos contra daños, lo cual actúa como un elemento 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 para los requisitos de seguridad:

a) la evaluación de los riesgos de la organización, teniendo en cuenta los objetivos y estrategia de negocio globales de la organización. A través de una evaluación de los riesgos se identifican las amenazas de los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su impacto potencial;

b) el conjunto de requisitos legales, estatutarios, regulatorios y contractuales que debería satisfacer la organización, sus socios comerciales, contratistas y proveedores de servicios, así como su entorno socio-cultural;

c) el conjunto de principios, objetivos y requisitos de negocio que la organización ha desarrollado para el manejo, tratamiento, almacenamiento, comunicación y archivo de la información que da soporte a sus operaciones.

Los recursos utilizados en la implantación de los controles han de estar equilibrados con el nivel de daños probables que resultarían de problemas de seguridad en ausencia de dichos controles. Los resultados de una evaluación de riesgos ayudarán a guiar y determinar las acciones de gestión más adecuadas y las prioridades para la gestión de los riesgos de seguridad de la información, así como para la implantación de los controles seleccionados para protegerse contra estos riesgos.

La Norma ISO/IEC 27005[11] facilita directrices sobre la gestión de los riesgos de seguridad de la información, incluyendo el asesoramiento sobre evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, vigilancia del riesgo y revisión del riesgo.

0.3 Selección de controles

Los controles pueden elegirse de los controles de esta norma o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cubrir adecuadamente las necesidades específicas.

La selección de los controles depende de las decisiones de carácter organizativo basadas en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y de los enfoques generales de gestión del riesgo aplicados en la organización, y debería depender también de toda la legislación y reglamentación nacional e internacional aplicable. La selección de los controles también depende del modo en que los controles interactúan para proporcionar una protección en profundidad.

Algunos de los controles en esta norma, pueden considerarse como principios que guían la gestión de la seguridad de la información, siendo aplicables a la mayoría de las organizaciones. Estos controles se explican con mayor grado de detalle más adelante junto con la guía de implementación de esta norma. Se puede encontrar más información sobre la selección de controles y otras posibilidades de tratamiento del riesgo en la Norma ISO/IEC 27005[11].

0.4 Desarrollo de directrices propias

Esta norma internacional puede verse como un punto de partida para desarrollar unas directrices específicas para la organización. Pueden no ser aplicables todas las recomendaciones y controles de este código de prácticas. Incluso, pueden requerirse controles adicionales que esta norma no incluye. Cuando esto suceda puede ser útil mantener referencias cruzadas de los capítulos de esta norma con otros documentos que contengan directrices adicionales de controles, que faciliten la comprobación del cumplimiento a los auditores y a otros socios de la organización.

0.5 Consideraciones del ciclo de vida

La información tiene un ciclo de vida natural, desde la creación y el origen de la misma pasando por el almacenamiento, tratamiento, utilización y transmisión hasta su eventual destrucción o deterioro. El valor y los riesgos para los activos puede variar durante su tiempo de vida (por ejemplo, la difusión no autorizada o el robo de las cuentas financieras de una empresa es mucho menos importante después de que hayan sido publicados oficialmente), pero la seguridad de la información continua siendo importante en todas las etapas.

Los sistemas de información tienen ciclos de vida en los cuales son concebidos, especificados, diseñados, desarrollados, probados, implantados, utilizados, mantenidos y, finalmente, retirados del servicio y eliminados. La seguridad de la información debería ser tenida en cuenta en todas estas etapas. Los nuevos desarrollos del sistema y los cambios en los sistemas actuales presentan oportunidades para que las organizaciones actualicen y mejoren los controles de seguridad, teniendo en cuenta tanto los incidentes reales como los riesgos de seguridad asociados a incidentes actuales y futuros.

0.6 Normas relacionadas

Aunque esta norma ofrece orientación sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones diferentes, las restantes Normas de la familia ISO/IEC 27000 proporcionan recomendaciones o requisitos complementarios sobre otros aspectos del proceso global de gestión de la seguridad de la información.

Se recomienda acudir a la Norma ISO/IEC 27000 para una introducción general tanto a los SGSI como a la familia de normas. La Norma ISO/IEC 27000 proporciona un glosario que define formalmente la mayoría de los términos utilizados en la familia de Normas ISO/IEC 27000, y describe el alcance y los objetivos para cada documento de la familia.

1 Objeto y campo de aplicación

Esta norma internacional establece directrices para la seguridad de la información en las organizaciones y prácticas de gestión de la seguridad de la información incluyendo la selección, la implantación, y la gestión de los controles teniendo en consideración el entorno de riesgos de seguridad de la información de la organización.

Esta norma internacional está diseñada para ser utilizada en organizaciones que pretendan:

a) seleccionar controles en el proceso de implantación de un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001[10];

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

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

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluyendo cualquier modificación de ésta).

ISO/IEC 27000, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.*

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma ISO/IEC 27000.

4 Estructura de esta norma

Esta norma consta de 14 capítulos de controles de seguridad que contienen un total de 35 categorías principales de seguridad y 114 controles.

4.1 Capítulos

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

El orden de los capítulos de esta norma no implica un orden de importancia. En función de las circunstancias, todos los controles de seguridad pueden ser importantes, por lo tanto cada organización que aplique esta norma debería identificar qué controles le son aplicables, cómo son de importantes y su aplicación a cada proceso de negocio. Asimismo, el orden de la lista de controles de esta norma no implica orden de prioridad.

4.2 Categorías de controles

Cada categoría principal de controles de seguridad contiene:

a) un objetivo del control que establece qué es lo que se quiere conseguir; y

b) uno o más controles que pueden ser aplicados para conseguir el objetivo del control.

Las descripciones de cada control se estructuran de la siguiente manera:

Control

Define la declaración del control específico para conseguir el objetivo del control.

Guía de implantación

Proporciona información más detallada para dar apoyo a la implantación del control y la consecución del objetivo del control. Algunas de estas directrices pueden no ser apropiadas o suficientes para todos los casos, pudiendo no adecuarse a los requisitos de control específicos para la organización.

Información adicional

Proporciona información adicional, cuya consideración puede ser necesaria, por ejemplo consideraciones legales y referencias a otras normas. Si no existe información adicional este apartado no se incluye.

5 Políticas de seguridad de la información

5.1 Directrices de gestión de la seguridad de la información

Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.

5.1.1 Políticas para la seguridad de la información

Control

Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Guía de implantación

Las organizaciones deberían definir una "política de seguridad de la información" al máximo nivel que sea aprobada por la dirección y establezca el enfoque de la organización para gestionar sus objetivos de seguridad de la información.

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

a) la estrategia de negocio;

b) la normativa, legislación y contratos;

c) el entorno actual y previsto de amenazas para la seguridad de la información.

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

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

b) la asignación de responsabilidades generales y específicas en materia de gestión de la seguridad de la información, para los roles definidos;

c) los procesos para el tratamiento de desviaciones y excepciones.

A un nivel inferior, la política de seguridad de la información debería apoyarse en políticas sobre temas específicos que profundicen en la implantación de controles y que, por lo general, estén estructuradas para atender las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas.

Ejemplos de estas políticas temáticas incluyen:

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

b) clasificación de la información (y su manejo) (véase 8.2);

c) seguridad física y ambiental (véase el capítulo 11);

d) temas orientados al usuario final tales como:

   1) uso adecuado de activos (véase 8.1.3),

   2) puesto de trabajo despejado y pantalla limpia (véase 11.2.9),

   3) transferencia de información (véase 13.2.1),

   4) dispositivos móviles y teletrabajo (véase 6.2),

   5) restricciones de instalación y uso de software (véase 12.6.2);

e) copias de respaldo (véase 12.3);

f) transferencia de información (véase 13.2);

g) protección ante el software malicioso (*malware*) (véase 12.2);

h) gestión de vulnerabilidades técnicas (véase 12.6.1);

i) controles criptográficos (véase el capítulo 10);

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

k) privacidad y protección de la información identificativa de personas (véase 18.1.4);

l) relaciones con proveedores (véase el capítulo 15).

Estas políticas deberían ser comunicadas a los empleados y terceras partes relevantes de una forma que sea apropiada, entendible y accesible al lector al que va dirigida, por ejemplo en el contexto de un "programa de concienciación, formación y educación en seguridad de la información" (véase 7.2.2).

Información adicional

La necesidad de políticas internas de seguridad de la información varía entre las organizaciones. Las políticas internas son especialmente útiles en las organizaciones grandes y complejas en las que los que definen y aprueban los niveles esperados de control son distintos de aquellos que implantan los controles, así como en situaciones en las cuales una política se aplica a muchas personas o a funciones diferentes en la organización. Las políticas para la seguridad de la información se pueden incluir en un solo documento de "política de seguridad de la información" o como un conjunto de documentos individuales, pero relacionados entre sí.

Si cualquiera de las políticas de seguridad de la información es distribuida al exterior de la organización, se debería tener cuidado en no revelar información confidencial.

Algunas organizaciones utilizan otros términos para estos documentos de política, tales como "Normas", "Directivas" o "Reglas".

5.1.2 Revisión de las políticas para la seguridad de la información

Control

Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Guía de implantación

Cada política debería tener un propietario a quien la dirección le ha asignado la responsabilidad de su desarrollo, revisión y evaluación. La revisión debería incluir la evaluación de oportunidades de mejora de las políticas de seguridad y un enfoque de cómo gestionar la seguridad de la información en respuesta a los cambios del entorno de la organización, de las circunstancias del negocio, de las condiciones legales, reglamentarias o contractuales o del entorno técnico.

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

Se debería obtener la aprobación de la dirección a la política revisada.

6 Organización de la seguridad de la información

6.1 Organización interna

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

6.1.1 Roles y responsabilidades en seguridad de la información

Control

Todas las responsabilidades en seguridad de la información deberían definirse y asignarse.

Guía de implantación

La asignación de responsabilidades relativas a seguridad de la información debería realizarse de acuerdo con las políticas de seguridad de la información (véase 5.1.1). Deberían identificarse las responsabilidades para la protección de activos individuales así como para llevar a cabo procesos de seguridad específicos. Deberían definirse las responsabilidades para las actividades de gestión de riesgos de seguridad de la información y, en particular, para la aceptación de riesgos residuales. Estas responsabilidades deberían completarse, dónde sea necesario, con una guía más detallada para ubicaciones e instalaciones de tratamiento de información específicas. Se deberían definir las responsabilidades locales para la protección de los activos y para llevar a cabo procesos de seguridad específicos.

Aquellos individuos a los que se les han asignado responsabilidades de seguridad pueden delegar estas tareas de seguridad en otros. Sin embargo, los primeros mantienen la responsabilidad y deberían comprobar que todas las tareas delegadas han sido correctamente realizadas.

Aquellas áreas para las que los individuos tienen asignadas responsabilidades deberían quedar establecidas, en particular en relación a los siguientes aspectos:

a) deberían identificarse y definirse los activos y los procesos de seguridad de la información;

b) debería asignarse una entidad responsable para cada activo o proceso de seguridad de la información y deberían documentarse los detalles de dicha responsabilidad (véase 8.1.2);

c) deberían definirse y documentarse los niveles de autorización;

d) para ser capaces de completar las responsabilidades en un área de seguridad de la información, los individuos designados deberían ser competentes en el área y tener la oportunidad de mantenerse actualizados en sus desarrollos;

e) deberían identificarse y documentarse los aspectos de coordinación y supervisión de seguridad de la información relativos a las relaciones con los proveedores.

Información adicional

En muchas organizaciones se nombra un responsable de seguridad de la información para asumir la responsabilidad general del desarrollo e implantación de la seguridad de la información y para dar soporte a la identificación de los controles.

Sin embargo, la responsabilidad de la provisión e implantación de los controles a menudo permanece en directivos a título individual. Una práctica común es nombrar un propietario para cada activo quien se hace responsable de la protección en el día a día.

6.1.2 Segregación de tareas

Control

Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Guía de implantación

Se debería cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte. El lanzamiento de un evento debería separarse de su autorización. Se debería considerar la posibilidad de connivencia en el diseño de los controles.

Las organizaciones pequeñas pueden considerar que la segregación de tareas es difícil de conseguir, pero el principio debería aplicarse en la medida en que sea posible y practicable. Cuando la segregación sea difícil, se deberían considerar otros controles como la monitorización de las actividades, las pistas de auditoría y la supervisión por la dirección.

Información adicional

La segregación de tareas es un método para reducir el riesgo de uso incorrecto de los activos de una organización, ya sea accidental o intencionado.

6.1.3 Contacto con las autoridades

Control

Deberían mantenerse los contactos apropiados con las autoridades pertinentes.

Guía de implantación

Las organizaciones deberían tener implantados procedimientos que especifiquen cuándo y con qué autoridades se debería contactar (por ejemplo, las autoridades encargadas de vigilar el cumplimiento de la legislación como las autoridades reguladoras y autoridades de supervisión y la manera adecuada de cómo y cuándo se debería informar de los incidentes de seguridad de la información (por ejemplo si se sospecha que se puede haber infringido la ley).

Información adicional

Las organizaciones que sufran un ataque a través de Internet pueden necesitar de las autoridades para emprender alguna acción contra la fuente del ataque.

El mantenimiento de tales contactos puede ser un requisito para dar soporte a la gestión de los incidentes de seguridad de la información (véase el capítulo 16) o a la continuidad del negocio y a los planes de contingencia (véase el capítulo 17). Los contactos con las autoridades encargadas de vigilar el cumplimiento de la legislación son también útiles para anticiparse y prepararse para los cambios que vendrán en nuevas leyes o reglamentaciones y que la organización tendrá que cumplir. Los contactos con otras autoridades, incluyen las empresas de servicios públicos, suministro eléctrico, servicios de emergencias, de seguridad y salud como, por ejemplo, cuerpos de bomberos (en relación a la continuidad del negocio), proveedores de servicios de telecomunicación (en relación con la disponibilidad y enrutamiento del servicio) y compañías de suministro de agua (en relación con las instalaciones de refrigeración para los equipos).

6.1.4 Contacto con grupos de interés especial

Control

Deberían mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

Guía de implantación

La participación como miembro en grupos de interés especial o foros debería ser considerado como medio para:

a) mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado sobre información relevante de seguridad;

b) asegurar un entendimiento, del entorno de seguridad de la información, actual y completo;

c) recibir avisos tempranos de alertas, asesoramiento y parches correspondientes a los ataques y las vulnerabilidades;

d) obtener acceso a asesoramiento especializado en seguridad de la información;

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

f) proporcionar adecuados puntos de enlace relacionados con incidentes de seguridad de la información (véase el capítulo 16).

Información adicional

Se pueden establecer acuerdos de intercambio de información para mejorar la cooperación y coordinación en los asuntos de seguridad. Tales acuerdos deberían identificar los requisitos para proteger la información confidencial.

6.1.5 Seguridad de la información en la gestión de proyectos

Control

La seguridad de la información debería tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

Guía de implantación

La seguridad de la información debería integrarse en el método o métodos de gestión de proyectos de la organización para asegurar que los riesgos de seguridad de la información se identifican y se contemplan en el marco de un proyecto. Esto se aplica en general a cualquier proyecto, independientemente de su carácter, por ejemplo, un proyecto para un proceso clave de negocio, de TI, de gestión de instalaciones y otros procesos de apoyo. Los métodos de gestión de proyectos en uso deberían exigir que:

a) los objetivos de seguridad de la información estén incluidos en los objetivos del proyecto;

b) se realiza una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar los controles necesarios;

c) la seguridad de la información es parte de todas las fases de la metodología aplicada en el proyecto.

Deberían contemplarse y revisarse con regularidad las implicaciones de seguridad de la información en todos los proyectos. Las responsabilidades de seguridad de la información deberían estar definidas y asignadas a los roles específicos señalados en los métodos de gestión de proyectos.

6.2 Los dispositivos móviles y el teletrabajo

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

6.2.1 Política de dispositivos móviles

Control

Se debería adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

Guía de implantación

Cuando se utilicen dispositivos móviles, se debería tener un cuidado especial para asegurar que no se compromete la información del negocio. La política de dispositivos móviles debería tener en cuenta los riesgos de trabajar con dispositivos móviles en entornos desprotegidos.

La política de dispositivos móviles debería considerar:

a) el registro de dispositivos móviles;

b) los requisitos para la protección física;

c) las restricciones de instalación de software;

d) los requisitos para las versiones de software de dispositivos móviles y para la aplicación de los parches y actualizaciones del software.

e) las restricciones de conexión a servicios de información;

f) los controles de acceso;

g) las técnicas criptográficas;

h) la protección ante el software malicioso (*malware*);

i) la inhabilitación, el borrado y bloqueo remotos;

j) las copias de respaldo;

k) la utilización de servicios y aplicaciones web.

Se debería tener cuidado con el uso de dispositivos móviles en zonas públicas, salas de reunión y otras áreas desprotegidas fuera de las instalaciones de la organización. Se debería implantar algún tipo de protección para evitar el acceso no autorizado o la revelación de la información almacenada y procesada por estos dispositivos, por ejemplo, utilizando técnicas criptográficas (véase el capítulo 10) e imponiendo el uso de protocolos secretos de identificación y autenticación (véase 9.2.4).

Los dispositivos móviles también deberían estar físicamente protegidos contra el robo, especialmente cuando se dejan, por ejemplo, en coches y otras formas de transporte, habitaciones de hoteles, centros de conferencia y lugares de reunión. Se debería establecer un procedimiento específico, que tuviera en cuenta, los requisitos legales, los requisitos de los seguros y otros requisitos de seguridad de la organización, para los casos de robo o pérdida de los dispositivos móviles. Los equipos que contengan información importante, sensible o crítica para el negocio, no se deberían dejar desatendidos y, cuando sea posible, se deberían bloquear físicamente, o se deberían utilizar cierres especiales para proteger el equipo.

Se debería proporcionar formación al personal que utiliza dispositivos móviles para aumentar su concienciación respecto a los riesgos adicionales de esta forma de trabajo y de los controles que se deberían implantar.

Cuando la política de dispositivos móviles permita el uso de dispositivos móviles personales o privados, la política y las medidas de seguridad relacionadas deberían considerar también:

a) la separación del uso de los dispositivos con fines privados respecto a los del negocio, incluyendo el uso de software para permitir dicha separación y proteger los datos de negocio en un dispositivo personal o privado;

b) proporcionar acceso a la información de la organización sólo después de que los usuarios han firmado un acuerdo de usuario final que incluya el reconocimiento de sus obligaciones (protección física, actualización de software, etc.), con renuncia a la propiedad de los datos de negocio, permitiendo la limpieza remota de los datos por la organización en caso de robo o pérdida del dispositivo o cuando ya no estén autorizados a utilizar el servicio. Esta política debería tener en cuenta la legislación de privacidad.

Información adicional

Las conexiones de dispositivos móviles a redes inalámbricas son similares a otros tipos de conexión a redes, pero tienen diferencias importantes que deberían tenerse en cuenta cuando se identifican los controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbrica son inmaduros y tienen debilidades;

b) de la información almacenada en dispositivos móviles puede que no se haga una copia de respaldo debido a la limitación del ancho de banda o porque el equipo móvil puede no estar conectado en el momento en que se programan las copias de seguridad.

Los dispositivos móviles, en general, comparten funciones comunes con los dispositivos de uso fijo como, por ejemplo, redes compartidas, acceso a Internet, correo electrónico y gestión de archivos. Los controles de seguridad de la información para los dispositivos móviles consisten, en general, en aquellos adoptados para los dispositivos de uso fijo y aquellos que hacen frente a las amenazas planteadas por su uso fuera de los locales de la organización.

6.2.2 Teletrabajo

Control

Se debería implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Guía de implantación

Las organizaciones que autorizan actividades de teletrabajo deberían instrumentar una política que defina las condiciones y restricciones para el uso del teletrabajo. Cuando se considere aplicable y permitido por la ley se deberían considerar los siguientes aspectos:

a) la existencia de seguridad física en el lugar de teletrabajo, teniendo en cuenta la seguridad física del edificio 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 va a acceder y transmitir a través del enlace de comunicación, así como la sensibilidad del sistema interno;

d) la facilitación de un acceso al escritorio virtual que prevenga el tratamiento y almacenamiento de información en equipos de uso personal o privado;

e) la amenaza de un intento de acceso no autorizado a la información o a los recursos por parte de otras personas del mismo emplazamiento, por ejemplo, familia y amigos;

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

g) las políticas y procedimientos para prevenir las disputas relativas a los derechos de propiedad intelectual de lo desarrollado por el propietario del equipo de manera privada;

h) el acceso a la parte privada del propietario del equipo (para comprobar la seguridad de la máquina o durante una investigación), que puede estar impedido por la legislación;

i) acuerdos de licencia de software que pueden hacer que las organizaciones puedan ser responsables de licenciar software cliente en los puestos de trabajo propiedad privada de empleados, contratistas o terceros;

j) los requisitos de protección frente a software malicioso (*malware*) y de cortafuegos.

Las directrices y disposiciones a ser consideradas deberían incluir:

a) la provisión del equipo adecuado y del mobiliario de almacenamiento para las actividades de teletrabajo, donde no se permita el uso de equipos privados que no estén bajo el control de la organización;

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

c) la provisión de los equipos de comunicación adecuados, incluyendo los métodos para asegurar el acceso remoto;

d) la seguridad física;

e) las reglas y directrices para el acceso de la familia y los accesos de los visitantes al equipo y a la información;

f) la provisión de soporte y mantenimiento de hardware y software;

g) la provisión de seguros;

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

i) auditoría y monitorización de la seguridad;

j) la revocación de la autorización y de los derechos de acceso, y la devolución del equipo cuando se terminan las actividades de teletrabajo.

Información adicional

El teletrabajo se refiere a todas las formas de trabajo fuera de la oficina, incluyendo entornos de trabajo no tradicionales tales como aquellos denominados "trabajo a distancia", "lugar de trabajo flexible", "trabajo en remoto" y "entornos virtuales de trabajo".

7 Seguridad relativa a los recursos humanos

7.1 Antes del empleo

Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

7.1.1 Investigación de antecedentes

Control

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debería ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.

Guía de implantación

Las comprobaciones deberían tener en cuenta la legislación relativa a privacidad, protección de datos personales y legislación laboral, y deberían, cuando esté permitido, incluir lo siguiente:

a) la disponibilidad de referencias satisfactorias, por ejemplo, una de tipo personal y otra profesional;

b) la comprobación (de la completitud y precisión) del currículum vitae del candidato;

c) la confirmación de las cualificaciones académicas y profesionales alegadas;

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

e) otras comprobaciones más detalladas, tales como comprobaciones crediticias y de antecedentes criminales.

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

a) tiene la competencia necesaria para desarrollar su rol en seguridad;

b) es confiable para asumir dicho perfil, especialmente si su desempeño es crítico para la organización.

Cuando un puesto de trabajo, ya sea un nombramiento inicial o una promoción, involucre que una persona tenga acceso a las instalaciones de tratamiento de la información, y en particular si se trata del manejo de información sensible, por ejemplo, información financiera o información altamente confidencial, la organización debería considerar realizar además otras comprobaciones más detalladas.

Los procedimientos deberían definir los criterios y limitaciones de las comprobaciones, por ejemplo, quién es candidato a una investigación de sus antecedentes, y cómo, cuándo y porque se llevan a cabo las comprobaciones.

Debería llevarse a cabo un proceso de investigación de antecedentes de los contratistas y de los terceros. En estos casos, el contrato entre la organización y el contratista debería especificar de una manera clara todas las responsabilidades y la notificación de los procedimientos relativos a la investigación de los antecedentes así como los procedimientos de notificación que es necesario seguir si la investigación no ha sido completada o si los resultados originan duda o inquietud.

La información de todos los candidatos que están siendo considerados para ocupar puestos dentro de la organización debería ser recopilada y tratada de acuerdo con la legislación aplicable existente en la jurisdicción correspondiente. Dependiendo de la legislación aplicable, los candidatos deberían ser informados con antelación sobre las actividades de investigación.

7.1.2 Términos y condiciones del empleo

Control

Cómo parte de sus obligaciones contractuales, los empleados y contratistas deberían establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

Guía de implantación

Los términos y condiciones del contrato de trabajo deberían reflejar la política de seguridad de la organización, además de establecer y clarificar lo siguiente:

a) que los empleados, contratistas y terceros que tengan acceso a información sensible, deberían firmar un compromiso de confidencialidad y no revelación previamente a que se les de el acceso a los recursos de tratamiento de la información (véase 13.2.4);

b) las responsabilidades y los derechos legales de los empleados y contratistas, por ejemplo, en relación a la legislación sobre derechos de propiedad intelectual o de protección de datos (véanse 18.1.2 y 18.1.4);

c) las responsabilidades para la clasificación de la información y la gestión de la información de la organización y de otros activos asociados a la información, a los recursos de tratamiento de la información y a los servicios de información manejados por el empleado o contratista (véase el capítulo 8);

d) las responsabilidades del empleado o contratista, relativas al manejo de la información recibida de otras compañías o de partes externas;

e) las acciones a tomar en caso de hacer caso omiso de los requisitos de seguridad de la organización por parte del empleado o contratista (véase 7.2.3).

Las responsabilidades y roles de seguridad de la información deberían comunicarse a los candidatos participantes en los procesos de selección de manera previa a la contratación.

La organización debería asegurar que los empleados y contratistas aceptan los términos y condiciones concernientes a la seguridad de la información que serán adecuadas a la naturaleza y extensión del acceso que tendrán a los activos de información asociados con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones del puesto de trabajo debería continuar durante un periodo de tiempo definido después de la finalización de la contratación (véase 7.3).

Información adicional

Se puede utilizar un código de conducta para cubrir las responsabilidades del empleado o contratista, relativas a la confidencialidad, protección de datos, ética, uso adecuado de los equipos y recursos de la organización, así como las prácticas profesionales que se esperan por la organización. El contratista o el tercero pueden estar vinculados con una organización externa que puede a su vez, requerir el establecer compromisos contractuales en nombre del individuo contratado.

7.2 Durante el empleo

Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.

7.2.1 Responsabilidades de gestión

Control

La dirección debería exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

Guía de implantación

Las responsabilidades de la dirección deberían incluir el garantizar que empleados y contratistas:

a) están debidamente informados sobre sus roles y responsabilidades relativas a seguridad de la información previamente a serles concedido el acceso a información sensible o a los sistemas de información;

b) se les proporcionan directrices para establecer las expectativas en cuanto a seguridad de la información en lo relativo a su función dentro de la organización;

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

d) alcanzan un nivel de concienciación en seguridad de la información adecuado a sus funciones y responsabilidades dentro de la organización (véase 7.2.2);

e) aceptan los términos y condiciones de su contratación, lo que incluye la política de seguridad de la información de la organización y los métodos de trabajo apropiados;

f) continúan teniendo el perfil profesional y las cualificaciones apropiados y son formados de manera regular;

g) disponen de un canal anónimo para reportar posibles violaciones de las políticas o procedimientos de seguridad de la información ("*whistle blowing*").

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

Información adicional

Si los empleados, contratistas y terceros, no son conscientes de sus responsabilidades en cuanto a seguridad de la información, podrían causar un daño considerable a la organización. El personal motivado es probablemente más fiable y causa menos incidentes de seguridad de la información.

Una gestión deficiente puede provocar que el personal se sienta infravalorado lo que tendría como resultado un impacto negativo en la seguridad de la organización. Por ejemplo, una gestión deficiente puede provocar descuidos en la seguridad o un posible mal uso de los activos de la organización.

7.2.2 Concienciación, educación y capacitación en seguridad de la información

Control

Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

Guía de implantación

Un programa de concienciación en seguridad de la información debería tener como objetivo el hacer a todos los empleados y, cuando corresponda, a los contratistas, tomar conciencia de sus responsabilidades en materia de seguridad de la información y los medios disponibles para ejercerla.

Un programa de concienciación en seguridad de la información debería estar alineado con las políticas y procedimientos de seguridad más relevantes, teniendo en cuenta qué información de la organización debería ser protegida y los controles que han sido implantados para protegerla. El programa de concienciación debería incluir un conjunto de actividades tales como campañas (por ejemplo, un "día de la seguridad de la información") y la elaboración de folletos y boletines.

El programa de concienciación debería diseñarse de acuerdo con la función de cada empleado en la organización y, cuando corresponda, las expectativas sobre el grado de concienciación de los contratistas. Las actividades incluidas en el programa de concienciación se deberían programar en el tiempo, preferentemente con una determinada regularidad, de manera que las actividades se repitan y den cobertura a los nuevos empleados y contratistas. El programa de concienciación también debería actualizarse regularmente para que se mantenga en línea con las políticas y procedimientos de la organización, y debería basarse en las lecciones aprendidas sobre de los incidentes de seguridad de la información.

La formación sobre concienciación se debería realizar según se establezca por el programa de concienciación, en seguridad de información de la organización. La formación sobre concienciación puede utilizar diferentes medios, incluyendo formación presencial, a distancia, basada en la web, autoaprendizaje y otros medios.

La formación y capacitación en seguridad de la información debería cubrir aspectos generales tales como:

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

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

c) la responsabilidad personal por las propias acciones y omisiones, y las responsabilidades generales relativas a asegurar o proteger la información que pertenece a la organización y a terceras partes;

d) los procedimientos básicos de seguridad de la información (tales como la notificación de incidentes de seguridad de la información) y los controles básicos (tales como la seguridad de las contraseñas, los controles de software malicioso (*malware*) y mesas despejadas);

e) los puntos de contacto y los recursos de información y consejos adicionales sobre cuestiones de seguridad de la información, que incluyan materiales adicionales para profundizar en la capacitación y formación en seguridad de la información.

La capacitación y formación en seguridad de la información deberían tener carácter periódico. La capacitación y la formación iniciales se aplican a aquellos que son transferidos a nuevos puestos o roles en la organización con requisitos sustancialmente diferentes de seguridad de la información, no sólo a las nuevas incorporaciones y siempre con antelación a la activación de una nueva función.

La organización debería desarrollar el programa de capacitación y formación con el fin de llevar a cabo una capacitación y formación eficaces. El programa debería estar en consonancia con las políticas y los procedimientos relevantes de seguridad de la información de la organización, teniendo en cuenta la información de la organización que ha de protegerse y los controles que se han implantado para proteger dicha información. El programa debería tener en cuenta las diferentes formas de capacitación y formación como, por ejemplo, conferencias o autoaprendizaje.

Información adicional

Al elaborar un programa de concienciación resulta importante no sólo centrarse en el "qué" y "cómo", sino también en el "por qué". Es importante que los empleados entiendan el propósito de la seguridad de la información y el impacto potencial, positivo y negativo, sobre la organización que tiene su propio comportamiento.

La concienciación, capacitación y formación pueden ser parte de, o llevarse a cabo en colaboración con, otras actividades de formación como, por ejemplo, tecnologías de la información o seguridad en general. Las actividades de concienciación, capacitación y formación deberían ser adecuadas y pertinentes a las funciones, responsabilidades y competencias del individuo.

Podría realizarse una evaluación del grado de comprensión alcanzado por los empleados al final de una actividad de concienciación, capacitación y formación para determinar el nivel de asimilación de los conocimientos transferidos.

7.2.3 Proceso disciplinario

Control

Debería existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

Guía de implantación

El proceso disciplinario no debería comenzar sin una previa verificación de que se ha producido una violación de la seguridad (véase 16.1.7).

El proceso disciplinario formal debería asegurar un tratamiento correcto e imparcial para los empleados de los que se sospeche hayan cometido alguna violación de la seguridad. El proceso disciplinario formal debería proporcionar una respuesta gradual que tenga en cuenta factores tales como la naturaleza y gravedad de la violación de la seguridad y su impacto en el negocio, si es la primera vez o se trata de una infracción repetida, si el causante fue adecuadamente formado, o no lo fue, en la legislación aplicable, los compromisos del negocio u otros factores según sea necesario.

El proceso disciplinario también debería ser utilizado como un elemento de disuasión para evitar que los empleados violen las políticas y procedimientos de seguridad de la información de la organización y demás violaciones de la seguridad de la información. Las infracciones deliberadas pueden requerir acciones inmediatas.

Información adicional

El proceso disciplinario puede también convertirse en una motivación o un incentivo si se definen recompensas para un comportamiento notable con respecto a la seguridad de la información.

7.3 Finalización del empleo o cambio en el puesto de trabajo

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

7.3.1 Responsabilidades ante la finalización o cambio

Control

Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deberían definir, comunicar al empleado o contratista y se deberían cumplir.

Guía de implantación

La comunicación de las responsabilidades en el cese debería incluir los requisitos de seguridad y las responsabilidades legales en curso, y cuando sea apropiado, las responsabilidades que conlleven algún acuerdo de confidencialidad (véase 13.2.4), así como los términos y condiciones del empleo (véase 7.1.2) que continúen durante un periodo definido después de la finalización del contrato del empleado o del contratista.

Las responsabilidades y funciones que son válidas después de la finalización del empleo deberían estar recogidas en los contratos de los empleados o contratistas (véase 7.1.2).

Los cambios de responsabilidad o de puesto de trabajo deberían ser gestionados de igual manera que la finalización de la responsabilidad o del empleo actual, y coordinamente con el inicio de la nueva responsabilidad o puesto de trabajo.

Información adicional

El departamento de Recursos Humanos generalmente es responsable del proceso completo de finalización y trabaja conjuntamente con el supervisor de la persona que deja su puesto para gestionar los aspectos de seguridad de los respectivos procedimientos. En el caso de un contratista proporcionado por una tercera parte, este proceso de finalización puede ser gestionado por ésta de acuerdo con lo establecido en el contrato entre la organización y la tercera parte.

Puede ser necesario informar a los empleados, clientes o contratistas, de los cambios de personal y los acuerdos de funcionamiento.

8 Gestión de activos

8.1 Responsabilidad sobre los activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

8.1.1 Inventario de activos

Control

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

Guía de implantación

La organización debería identificar los activos relevantes para el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, tratamiento, almacenamiento, transmisión, borrado y destrucción. La documentación debería ser mantenida en inventarios dedicados o existentes según lo que sea adecuado.

El inventario de activos debería ser preciso, estar actualizado, ser consistente y estar en consonancia con otros inventarios.

Cada uno de los activos identificados debería tener asignado un propietario (véase 8.1.2) e identificada su clasificación (véase 8.2).

Información adicional

Los inventarios de activos ayudan a asegurar que se ejerce una protección eficaz, y pueden ser necesarios para otros propósitos, tales como razones de seguridad y salud laboral, seguros patrimoniales y financieros (gestión de activos).

La Norma ISO/IEC 27005[11] proporciona ejemplos de activos que la organización puede necesitar considerar de cara a la identificación de activos. El proceso de compilar un inventario de activos es un prerrequisito importante para la gestión del riesgo (véase también las Norma ISO/IEC 27000 y ISO/IEC 27005[11]).

8.1.2 Propiedad de los activos

Control

Todos los activos que figuran en el inventario deberían tener un propietario.

Guía de implantación

Tanto individuos como otros órganos que hayan sido autorizados por la dirección como competencialmente aptos para la gestión del ciclo de vida de activos pueden ser designados como propietarios de activos.

Normalmente se implementa un proceso para asegurar la puntual asignación de propiedad sobre los activos. La propiedad debería asignarse bien al crearse los activos o bien cuando la organización los recibe. El propietario del activo debería ser responsable de la adecuada gestión del activo durante todo su ciclo de vida.

El propietario del activo debería:

a) asegurar que los activos son inventariados;

b) asegurar que los activos se clasifican y protegen debidamente;

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

d) asegurar el manejo adecuado para el borrado o destrucción del activo.

Información adicional

El propietario identificado puede ser tanto un individuo como un órgano que haya sido autorizado por la dirección como competencialmente apto para la gestión de todo el ciclo de vida del activo. El propietario identificado no tiene necesariamente que tener derechos de propiedad sobre el activo.

Las tareas rutinarias pueden delegarse, por ejemplo, a un custodio al cuidado diario de los activos, pero la responsabilidad permanece asignada al propietario.

En sistemas de información complejos, puede ser útil designar grupos de activos que interactúan en la producción de un servicio específico. En dicho caso, el propietario de dicho servicio responde de dar el servicio, incluyendo la operación de sus activos.

8.1.3 Uso aceptable de los activos

Control

Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

Guía de implantación

Debería concienciarse a los usuarios, tanto empleados como externos que usen o tengan acceso a los activos de la organización sobre los requisitos de seguridad de la información que afectan a la información de la organización, a otros activos asociados a la información y a los recursos de tratamiento de la información. Deberían ser responsables del uso que hagan de los recursos de tratamiento de información y cualquier otro uso hecho bajo su responsabilidad.

8.1.4 Devolución de activos

Control

Todos los empleados y terceras partes deberían devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

Guía de implantación

Debería estar formalizado un proceso de desvinculación que incluya la devolución de todo activo físico y electrónico que sean propiedad de la organización o estén bajo su custodia.

Cuando el usuario, sea empleado o externo, adquiere recursos para la organización o emplea sus propios recursos, deberían seguirse procedimientos para asegurar que toda la información relevante se devuelve a la organización y se borra definitivamente de dichos recursos (véase 11.2.7).

Cuando el usuario, sea empleado o externo, tenga conocimiento sobre asuntos importantes para las operaciones en curso, deberían documentarse dichos conocimientos y ser transferidos a la organización.

La organización debería controlar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) durante el periodo entre la notificación de desvinculación de personas y contratistas y la materialización efectiva de la misma.

8.2 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control

La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

Guía de implantación

Las clasificaciones de la información y controles de protección asociados deberían tener en consideración las necesidades de negocio en cuanto a compartir o restringir información, así como también los requisitos legales. Además de la información, otros activos pueden ser clasificados considerando la clasificación de la información que almacenan, procesan o cualquier otra forma de protección o tratamiento por el activo.

Los propietarios de los activos de información deberían ser responsables de su clasificación.

El esquema de clasificación debería incluir normas para la clasificación y los criterios de revisión de la clasificación en el tiempo. El nivel de protección en el esquema debería ser evaluado analizando los requisitos de confidencialidad, integridad y disponibilidad y cualquier otro para la información considerada. El esquema debería estar alineado con la política de control de acceso (véase 9.1.1).

Debería designarse cada nivel con un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.

El esquema debería ser consistente de manera transversal en toda la organización de forma que todas las personas clasifiquen la información y activos relacionados de la misma forma, tengan un entendimiento común de los requisitos de protección y apliquen la protección adecuada.

La clasificación debería formar parte de los procesos de la organización, y ser consistente y coherente de manera transversal en toda la organización. Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, por ejemplo, en términos de su confidencialidad, integridad y disponibilidad. Los resultados de la clasificación deberían actualizarse cuando cambie su valor, sensibilidad y criticidad a lo largo de su ciclo de vida.

Información adicional

La clasificación proporciona una indicación concisa sobre cómo debería tratarse y protegerse la información para las personas que tratan información. Esto se facilita con la creación de conjuntos de información con necesidades de protección similares y especificando qué procedimientos de seguridad de la información se aplican a toda la información de cada conjunto. Esta aproximación reduce la necesidad de evaluaciones del riesgo caso a caso y el diseño de controles a medida.

La información puede dejar de ser sensible o critica después de un periodo de tiempo, por ejemplo, cuando se ha difundido al público. Tales aspectos deberían ser considerados, ya que la clasificación excesiva puede conllevar a la implantación de controles innecesarios con un gasto adicional, o por el contrario una clasificación insuficiente puede poner en peligro el logro de objetivos de negocio.

Un ejemplo de esquema de clasificación de confidencialidad de la información podría basarse en cuatro niveles tales como:

a) la revelación no conlleva daños;

b) la revelación causa incomodidad menor o molestias operativas menores;

c) la revelación tiene un impacto significativo a corto plazo sobre operaciones u objetivos tácticos;

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

8.2.2 Etiquetado de la información

Control

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Guía de implantación

Los procedimientos de etiquetado de la información deberían contemplar la información y los activos relacionados tanto en soporte físico como electrónico. El etiquetado debería corresponderse con el esquema de clasificación establecido en 8.2.1. Las etiquetas deberían ser fácilmente reconocibles. Los procedimientos deberían proporcionar directrices sobre dónde y cómo se vinculan las etiquetas considerando como se accede a la información o como se tratan los activos dependiendo del tipo de soporte. Los procedimientos pueden definir casos dónde se prescinda del etiquetado, por ejemplo, en el etiquetado de activos no confidenciales para reducir la carga de trabajo. Debería concienciarse sobre los procedimientos de etiquetado tanto a empleados como a externos.

Deberían marcarse con una etiqueta adecuada los resultados producidos por sistemas que contengan información clasificada como sensible o critica.

Información adicional

El etiquetado de información clasificada es un requisito clave en los acuerdos de compartición de información. Etiquetas físicas y metadatos son formas corrientes de etiquetar.

El etiquetado de información y activos relacionados puede conllevar en ocasiones efectos negativos. Los activos clasificados son identificados más fácilmente y en consecuencia pueden ser robados con mayor facilidad por miembros de la organización o atacantes externos.

8.2.3 Manipulado de la información

Control

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Guía de implantación

Deberían redactarse procedimientos para el manejo, tratamiento, almacenado y comunicación de información consistentes con su clasificación (véase 8.2.1).

Los siguientes elementos deberían contemplarse:

a) restricciones de acceso que dan apoyo a los requisitos de protección para cada nivel de clasificación;

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

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

d) almacenamiento de activos de TI conforme a las especificaciones de sus fabricantes;

e) marcado claro en todas las copias de soportes para la debida atención del receptor autorizado.

El esquema de clasificación empleado por la organización puede no ser equivalente a los esquemas empleados por otras organizaciones, incluso si los nombres de los niveles son semejantes; además, la información que circula entre organizaciones puede variar su clasificación dependiendo de su contexto en cada organización, incluso si su nivel de clasificación es idéntico.

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

8.3 Manipulación de los soportes

Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

8.3.1 Gestión de soportes extraíbles

Control

Se deberían implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.

Guía de implantación

Deberían considerarse las directrices siguientes para la gestión de soportes extraíbles:

a) en caso de ya no ser necesarios, deberían borrarse definitivamente los contenidos de cualquier soporte reutilizable que vaya a ser retirado;

b) cuando sea necesario y práctico, debería solicitarse autorización para extraer soportes de la organización, y debería mantenerse un registro de tales retiradas para mantener la trazabilidad a efectos de auditoría;

c) todos los soportes deberían almacenarse en un entorno seguro y protegido, conforme a las especificaciones de sus fabricantes;

d) deberían emplearse técnicas criptográficas para proteger datos en soportes extraíbles en caso de que apliquen requisitos importantes de confidencialidad o integridad;

e) los datos deberían transferirse a soportes de fabricación reciente antes de que se conviertan en ilegibles, a fin de mitigar el riesgo de degradación del soporte durante el tiempo en que los datos almacenados aún son necesarios;

f) deberían almacenarse copias múltiples de datos valiosos en soportes separados para reducir aún más el riesgo de daño o pérdida simultánea de los datos;

g) el inventariado de soportes extraíbles debería considerarse para limitar las posibilidades de pérdida de datos;

h) solo deberían permitirse reproductores de soportes extraíbles cuando haya una razón de negocio para ello;

i) la transferencia de información a medios extraíbles debería ser monitorizada, cuando hay necesidad de usar dichos soportes.

Deberían documentarse los procedimientos y los niveles de autorización.

8.3.2 Eliminación de soportes

Control

Los soportes deberían eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

Guía de implantación

Deberían establecerse procedimientos formales para la eliminación segura de soportes, para minimizar el riesgo de filtraciones de información confidencial a personas no autorizadas. Los procedimientos para eliminación segura de soportes que contengan información confidencial deberían ser proporcionales a la sensibilidad de dicha información. Los siguientes elementos deberían considerarse:

a) aquellos soportes que contengan información confidencial deberían almacenarse y desecharse con seguridad, por ejemplo, por incineración o triturado, o mediante el borrado de datos para la reutilización de los soportes por la organización;

b) deberían implantarse procedimientos para identificar los elementos que requieran una eliminación segura;

c) puede ser más simple organizar la recolección y eliminación segura de todos los soportes en lugar de tratar de segregar elementos sensibles;

d) muchas organizaciones ofrecen servicios de recolección y eliminación de soportes, deberían tomarse cautelas en la selección de terceros externos apropiados, con la adecuada experiencia y controles;

e) la eliminación de elementos sensibles debería quedar registrado a fin de mantener trazabilidad para su auditoría.

Cuando se acumulen soportes para su eliminación, debería prestarse atención al efecto de acumulación, donde un conjunto de información no sensible puede convertirse en sensible por su cantidad.

Información adicional

Aquellos recursos dañados que contengan datos sensibles pueden requerir una evaluación del riesgo, a fin de determinar si los elementos deberían ser destruidos en lugar de ser reparados o simplemente descartados (véase 11.2.7).

8.3.3 Soportes físicos en tránsito

Control

Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

Guía de implantación

Deberían considerarse las siguientes directrices de cara a proteger soportes que contengan información durante su transporte:

a) debería emplearse un servicio fiable de transporte o mensajería;

b) debería acordarse con la dirección una lista de mensajeros autorizados;

c) deberían desarrollarse procedimientos para verificar la identidad de los mensajeros;

d) el embalaje debería proteger suficientemente el contenido de todo daño físico que pueda razonablemente ocurrir durante el tránsito, y conforme con las especificaciones de su fabricante por ejemplo protegiendo de factores ambientales que puedan reducir la eficacia de la recuperación del soporte tales como exposición al calor, polvo o campos electromagnéticos;

e) deberían mantenerse registros, identificando el contenido de los soportes, la protección aplicada, así como reflejando los momentos de transferencia a los custodios y la recepción en el destino.

Información adicional

La información puede ser vulnerable al acceso no autorizado, mal uso y corrupción durante su transporte físico, por ejemplo, al remitir soportes mediante correo postal o mensajeros. En este control, el papel es un soporte más.

Cuando la información contenida en los soportes sea confidencial y no esté cifrada, deberían tenerse en cuenta medidas de protección física adicionales.

9 Control de acceso

9.1 Requisitos de negocio para el control de acceso

Objetivo: Limitar el acceso a los recursos de tratamiento de información y a la información.

9.1.1 Política de control de acceso

Control

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

Guía de implantación

Los propietarios de los activos deberían determinar las reglas apropiadas para el control de acceso, los derechos y las restricciones de acceso a sus activos para los diferentes roles de usuarios, con el nivel de detalle y rigor de los controles que refleje los riesgos de seguridad de la información asociados.

Los controles de acceso son tanto lógicos como físicos (véase el capítulo 11) y deberían considerarse conjuntamente. Se debería proporcionar a los usuarios y proveedores de servicio una declaración clara de los requisitos de negocio a satisfacer por los controles de acceso.

La política debería tener en cuenta lo siguiente:

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

b) las políticas para la diseminación y autorización de la información, por ejemplo el principio de la 'necesidad de conocer' y los niveles de seguridad y de clasificación de la información (véase 8.2);

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

d) la legislación aplicable y cualquier obligación contractual relativa a la limitación de acceso a datos o servicios (véase 18.1);

e) la gestión de los derechos de acceso en un entorno distribuido e interconectado que reconozca todos los tipos de conexiones disponibles;

f) la segregación de las funciones en el control de acceso en diversos roles, por ejemplo la petición de acceso, la autorización de acceso, la administración de acceso;

g) los requisitos para la autorización formal de las peticiones de acceso (véase 9.2.1 y 9.2.2);

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

i) la retirada de los derechos de acceso (véase 9.2.6);

j) la conservación y registro de todos los eventos significativos con referencia al uso y gestión de la identidad de usuario y de la información secreta para la autenticación;

k) los roles con derechos de acceso privilegiados (véase 9.2.3).

Información adicional

Se debería considerar lo siguiente al especificar las reglas de control de acceso:

a) el establecimiento de reglas basadas en la premisa de "Todo está prohibido a no ser que se permita expresamente" en vez de la regla más débil "Todo está permitido a no ser que se prohíba expresamente";

b) los cambios en el etiquetado de la información (véase 8.2.2) que realizan automáticamente los recursos de tratamiento de la información y los iniciados a discreción del usuario;

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

d) las reglas que requieren aprobación específica previa a su promulgación y aquellas que no.

Las reglas de control de acceso deberían estar recogidas en procedimientos formales (véanse 9.2, 9.3, 9.4) y las responsabilidades deberían estar definidas (véanse 6.1.1, 9.3).

El control de acceso basado en roles es una aproximación utilizada con éxito por muchas organizaciones para vincular los derechos de acceso con las funciones desempeñadas en el negocio.

Dos de los principios frecuentemente recogidos en la política de control de acceso son:

a) "la necesidad de conocer": sólo se da acceso a aquella información necesaria para realizar las tareas (diferentes tareas/roles recogen diferentes 'necesidades de conocer' y por tanto diferentes perfiles de acceso);

b) "la necesidad de usar": sólo se da acceso a los recursos necesarios para el tratamiento de la información (equipos, aplicaciones, procedimientos, instalaciones de TI) para la realización de la tarea/trabajo/rol.

9.1.2 Acceso a las redes y a los servicios de red

Control

Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

Guía de implantación

Debería formularse una política para el uso de las redes y de los servicios de red. Esta política debería especificar:

a) las redes y los servicios de red a los que está permitido el acceso;

b) los procedimientos de autorización que determinen quién tiene permitido el acceso a qué redes y a qué servicios de red;

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

d) los medios usados para acceder a las redes o a los servicios de red (por ejemplo, el uso de VPNs – redes privadas virtuales – o de redes inalámbricas);

e) los requisitos de autenticación de usuarios para el acceso a varios servicios de red;

f) la monitorización del uso de los servicios de red.

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

Información adicional

Las conexiones a los servicios de red no autorizadas e inseguras pueden afectar al conjunto de la organización. Este control es particularmente importante para las conexiones de red a aplicaciones de negocio sensibles o críticas o para usuarios en lugares de alto riesgo, por ejemplo, en áreas públicas o áreas externas que están fuera de la gestión y control de la seguridad de la información de la organización.

9.2 Gestión de acceso de usuario

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

9.2.1 Registro y baja de usuario

Control

Debería implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

Guía de implantación

El proceso para la gestión de los identificadores (IDs) de usuario debería incluir:

a) el uso de identificadores (ID) de usuario únicos que le identifiquen y le hagan responsable de sus acciones; tan sólo debería permitirse el uso de identificadores (ID) compartidos cuando fuera necesario por razones del negocio o de operación y debería ser aprobado y quedar documentado;

b) la inhabilitación o eliminación inmediata de los identificadores (ID) de usuarios que dejan la organización (véase 9.2.6);

c) la identificación periódica y eliminación o inhabilitación de identificadores de usuario redundantes;

d) asegurar que no se dan identificadores de usuario redundantes a otros usuarios.

Información adicional

La provisión o la revocación del acceso a la información o a los recursos para su tratamiento consta habitualmente de dos fases:

a) la asignación y habilitación, o la revocación de un identificador (ID) de usuario;

b) la provisión o revocación de los derechos de acceso a ese identificador (ID) de usuario (véase 9.2.2).

9.2.2 Provisión de acceso de usuario

Control

Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

Guía de implantación

El proceso usado para la asignación o revocación de los derechos de acceso concedidos a los identificadores (ID) de usuario debería incluir:

a) obtener la autorización del propietario del sistema de información o del servicio para el uso de éste (véase el control 8.1.2); además, puede ser apropiada la aprobación adicional y por separado por parte de la dirección, de los derechos de acceso;

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

c) asegurar que los derechos de acceso no se activan (por ejemplo, por los proveedores de servicio) hasta concluir con los procedimientos de autorización;

d) mantener un registro central de derechos de acceso a sistemas de información y servicios concedidos a un identificador (ID) de usuario;

e) adaptar los derechos de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado la organización;

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

Información adicional

Se debería considerar el establecimiento de roles de acceso de usuario basados en los requisitos del negocio de forma que agrupen varios derechos de acceso en perfiles de acceso de usuario típicos. Las peticiones y la revisión de derechos de acceso (véase 9.2.4) son más fáciles de gestionar a nivel de roles que a nivel de derechos particulares.

Debería considerarse la inclusión de cláusulas en los contratos del personal y en los contratos de servicios que especifiquen las sanciones en caso de que el personal o los contratistas intenten realizar un acceso no autorizado (véase 7.1.2, 7.2.3, 13.2.4. 15.1.2).

9.2.3 Gestión de privilegios de acceso

Control

La asignación y el uso de privilegios de acceso debería estar restringida y controlada.

Guía de implantación

La asignación de derechos de acceso privilegiados debería estar controlada a través de un proceso formal de autorización de acuerdo con la política de control de acceso aplicable (véase 9.1.1). Los siguientes pasos deberían ser considerados:

a) deberían identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso, por ejemplo, sistema operativo, el sistema de gestión de base de datos y cada aplicación, junto con los usuarios a los que hay que asignarlos;

b) los derechos de acceso privilegiados deberían asignarse a los usuarios en base a la 'necesidad de uso' y caso a caso de acuerdo con la política de control de acceso (véase 9.1.1), es decir, basados en los requisitos mínimos para el desempeño de sus funciones;

c) debería mantenerse un proceso de autorización y registro de todos los privilegios asignados. Los derechos de acceso privilegiados no deberían concederse hasta que se complete el proceso de autorización;

d) deberían definirse los requisitos para el vencimiento de los derechos de acceso privilegiados;

e) los derechos de acceso privilegiados deberían asignarse a un identificador (ID) de usuario diferente al usado en las actividades normales del negocio. Las actividades normales del negocio no deberían ser ejecutadas desde un identificador (ID) privilegiado;

f) deberían revisarse regularmente las competencias de los usuarios con derechos de acceso privilegiados verificando que se correspondan con sus tareas;

g) deberían establecerse y mantenerse procedimientos específicos para evitar el uso no autorizado del identificador (ID) de usuario administrador genérico en relación con las capacidades de configuración de los sistemas;

h) para el identificador (ID) de usuario administrador genérico, debería mantenerse la confidencialidad de la información secreta de autenticación cuando éstos sean compartidos (por ejemplo, cambiando las contraseñas con frecuencia y tan pronto como sea posible cuando un usuario privilegiado deje la organización o cambie de trabajo, comunicándolas a los usuarios privilegiados a través de los mecanismos apropiados).

Información adicional

El uso inadecuado de privilegios de administrador del sistema (cualquier característica o recurso para el tratamiento de un sistema de información que permita al usuario anular los controles del sistema o aplicación) es un factor que contribuye de forma importante al fallo o a la violación de los sistemas.

9.2.4 Gestión de la información secreta de autenticación de los usuarios

Control

La asignación de la información secreta de autenticación debería ser controlada a través de un proceso formal de gestión.

Guía de implantación

El proceso debería incluir los siguientes requisitos:

a) se debería requerir a los usuarios la firma de un compromiso de mantener la confidencialidad de la información secreta para la autenticación personal y mantener la información de autenticación secreta del grupo (es decir, la compartida) entre los miembros del mismo; este compromiso firmado podría incluirse en los términos y condiciones del empleo (véase 7.1.2);

b) cuando se requiera a los usuarios mantener su información de autenticación secreta, debería proporcionárseles inicialmente una autenticación temporal a cambiar obligatoriamente en el primer uso;

c) deberían establecerse procedimientos para verificar la identidad de un usuario antes de proporcionarle la información de autenticación secreta ya sea nueva, de sustitución o provisional;

d) la información de autenticación secreta debería proporcionarse a los usuarios de manera segura; evitando el uso de terceras partes o de correos electrónicos no protegidos (texto sin cifrar);

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

f) los usuarios deberían confirmar la recepción de la información de autenticación secreta;

g) la información de autenticación secreta por defecto del vendedor, debería cambiarse tras la instalación de los sistemas o del software.

Información adicional

Las contraseñas son un tipo de información de autenticación secreta usado comúnmente para verificar la identidad de los usuarios. Otros tipos de información de autenticación secreta son las claves criptográficas y otros datos almacenados en dispositivos hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación.

9.2.5 Revisión de los derechos de acceso de usuario

Control

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

Guía de implantación

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

a) los derechos de acceso de usuario deberían revisarse a intervalos regulares y tras cualquier cambio, como una promoción, degradación o finalización del empleo (véase el capítulo 7);

b) los derechos de acceso de usuario deberían revisarse y reasignarse cuando éste cambie de rol dentro de la misma organización;

c) las autorizaciones de derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes;

d) la asignación de privilegios debería verificarse a intervalos regulares para asegurar que no se han obtenido privilegios no autorizados;

e) los cambios en cuentas privilegiadas deberían registrarse para su 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 Retirada o reasignación de los derechos de acceso

Control

Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.

Guía de implantación

Tras la finalización del empleo, los derechos de acceso de un individuo a la información y activos asociados con los recursos de tratamiento de la información y servicios deberían eliminarse o suspenderse. Esto determinará si es necesaria la eliminación de los derechos de acceso. Los cambios en el empleo deberían tener reflejo en la eliminación de todos los derechos de acceso que no fueran aprobados para el nuevo trabajo. Los derechos de acceso que deberían ser eliminados o ajustados incluyen tanto los de acceso físico como lógico. La eliminación o el ajuste puede hacerse eliminando, revocando o reemplazando claves, tarjetas de identificación, recursos de tratamiento de la información o subscripciones. Cualquier documentación que identifique los derechos de acceso de empleados y de contratistas debería reflejar la eliminación o ajuste de derechos de acceso. Si se conoce que el empleado o el usuario de una tercera parte que deja el puesto, posee contraseñas para identificadores de usuario que queden activos, estos deberían cambiarse tras la finalización o cambio en el contrato o acuerdo de trabajo.

Los derechos de acceso a la información y los activos asociados a los recursos de tratamiento de la información deberían restringirse o eliminarse antes que el empleado finalice o cambie de puesto de trabajo, dependiendo de la evaluación de factores de riesgo como:

a) si la finalización o el cambio de puesto de trabajo la inicia el empleado, el usuario de la tercera parte o la dirección, así como la razón para la finalización;

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

c) el valor de los activos accesibles en ese momento.

Información adicional

En ciertas circunstancias los derechos de acceso pueden asignarse de forma que estén disponibles para más usuarios aparte del empleado o el usuario de la tercera parte que se va, por ejemplo, en el caso de identificadores (ID) de grupo. En esas circunstancias, debería eliminarse su identificador de todas las listas de acceso de grupos y se deberían tomar medidas para informar a los demás empleados y a usuarios de terceras partes en la lista para que no compartan más esta información con el usuario que se va.

En los casos en que la finalización la inicia la dirección, los empleados o usuarios de tercera parte descontentos pueden corromper la información o sabotear los recursos para su tratamiento deliberadamente. Cuando las personas dimiten o son despedidas, pueden tener la tentación de recopilar información para su uso futuro.

9.3 Responsabilidades del usuario

Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.

9.3.1 Uso de la información secreta de autenticación

Control

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

Guía de implantación

Los usuarios deberían ser advertidos de:

a) mantener confidencial la información de autenticación, asegurando que no se divulgue a cualquier otra parte, incluyendo personas con autoridad;

b) evitar guardar (por ejemplo, en papel, en un fichero software o en un dispositivo portátil) la información secreta de autenticación, a no ser que ésta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, en repositorios seguros para contraseñas);

c) cambiar la información secreta de autenticación siempre que haya indicios de su posible compromiso;

d) cuando se usen contraseñas como información secreta de autenticación, seleccionar contraseñas de calidad con una longitud mínima suficiente que sean:

   1) fáciles de recordar,

   2) que no estén basadas en algo que alguien más pueda adivinar con facilidad u obtener usando información asociada a la persona, por ejemplo, nombres, números de teléfono, fechas de nacimiento, etc.,

   3) que no sea vulnerable a ataques de diccionario (es decir, que no consista en palabras incluidas en diccionarios),

   4) que estén libres de caracteres consecutivos bien sean todos numéricos o todos alfabéticos,

   5) si es temporal, que sea cambiada en el primer inicio de sesión,

e) no compartir la información secreta de autenticación individual del usuario;

f) asegurar una protección adecuada de las contraseñas cuando estas sean usadas como información secreta de autenticación y almacenadas en procesos automáticos de inicio de sesión;

g) no usar la misma información secreta de autenticación para propósitos laborales y no laborales.

Información adicional

La provisión de herramientas de autenticación única *Single Sign On* (SSO) u otras herramientas de gestión de la información secreta de autenticación reduce la cantidad de información secreta de autenticación que los usuarios deberían proteger, incrementando por consiguiente la efectividad de este control. Sin embargo, estas herramientas pueden incrementar también el impacto de la revelación de la información secreta de autenticación.

9.4 Control de acceso a sistemas y aplicaciones

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información

Control

Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

Guía de implantación

Las restricciones de acceso deberían basarse en los requisitos individuales de las aplicaciones de negocio y de acuerdo con la política de control de acceso definida.

Para apoyar los requisitos de restricción de acceso debería considerarse lo siguiente:

a) proporcionar menús para el control del acceso a las funciones del sistema de aplicaciones;

b) controlar qué datos pueden ser accedidos por un usuario determinado;

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

d) controlar los derechos de acceso de otras aplicaciones;

e) limitar la información contenida en las salidas del sistema;

f) proporcionar controles de acceso físico o lógico para aislar las aplicaciones sensibles, los datos de aplicación o los sistemas.

9.4.2 Procedimientos seguros de inicio de sesión

Control

Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debería controlar por medio de un procedimiento seguro de inicio de sesión.

Guía de implantación

Debería escogerse una técnica de autenticación adecuada para confirmar la identidad que reivindica el usuario.

Cuando se requiera una autenticación y verificación robusta de la identidad deberían usarse métodos de autenticación alternativos a las contraseñas, como por ejemplo, medios criptográficos, tarjetas inteligentes, dispositivos hardware o medios biométricos.

El procedimiento para iniciar la sesión en un sistema o aplicación debería diseñarse para minimizar la oportunidad de acceso no autorizado. El procedimiento de inicio de sesión debería, por tanto, revelar el mínimo de información sobre el sistema o la aplicación, para evitar proporcionar ayuda innecesaria a un usuario no autorizado. Un buen procedimiento de inicio de sesión debería:

a) no mostrar identificadores del sistema o aplicación hasta que el proceso de inicio de sesión se haya completado con éxito;

b) mostrar un aviso general de que únicamente deberían acceder al ordenador los usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el proceso de entrada que pudieran ayudar a un usuario no autorizado;

d) validar la información de inicio de sesión solo cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no debería indicar qué parte del dato es correcta o incorrecta;

e) proteger contra los intentos de fuerza bruta de inicio de sesión;

f) registrar los intentos con y sin éxito ocurridos;

g) generar un evento de seguridad cuando se detecte un intento potencial o con éxito de violación de los controles de inicio de sesión;

h) mostrar la siguiente información tras completar con éxito el inicio de sesión:

   1) fecha y hora del anterior inicio de sesión con éxito,

   2) los detalles de cualquier intento de inicio de sesión sin éxito desde el anterior con éxito,

i) no mostrar la contraseña que se está introduciendo;

j) no transmitir por la red contraseñas sin cifrar;

k) terminar las sesiones inactivas tras un periodo definido de inactividad, especialmente en lugares de alto riesgo, como áreas públicas o externas que queden fuera de la gestión de la seguridad de la organización o en dispositivos móviles;

l) restringir los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo y reduciendo la ventana de oportunidad de los usuarios no autorizados.

Información adicional

Las contraseñas son una forma común de proveer identificación y autenticación basadas en un secreto que tan sólo conoce el usuario. Puede conseguirse lo mismo con medios criptográficos y protocolos de autenticación. La fortaleza de la autenticación de usuario debería ser la apropiada para la clasificación de la información a la que se accede.

Si durante el inicio de sesión se trasmiten por la red las contraseñas sin cifrar, éstas pueden ser capturadas por un programa de "escucha" (*sniffer*) de la red.

9.4.3 Sistema de gestión de contraseñas

Control

Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas.

Guía de implantación

Un sistema de gestión de contraseñas debería:

a) aplicar el uso de identificadores (ID) de usuario y contraseñas individuales para mantener la responsabilidad;

b) permitir a los usuarios escoger y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada;

c) imponer la selección de contraseñas de calidad;

d) forzar a los usuarios a cambiar sus contraseñas tras el primer inicio de sesión;

e) forzar los cambios regulares de contraseñas y bajo petición;

f) mantener un registro de las contraseñas usadas anteriormente y evitar su reutilización;

g) no mostrar las contraseñas en la pantalla cuando se estén introduciendo;

h) almacenar los ficheros de contraseñas de manera separada de los datos del sistema de aplicación;

i) almacenar y transmitir las contraseñas en forma protegida.

Información adicional

Algunas aplicaciones requieren que las contraseñas de usuario sean asignadas por una autoridad independiente; en tales casos los puntos b), d) y e) de la guía anterior no son de aplicación. En la mayoría de los casos las contraseñas son escogidas y mantenidas por los usuarios.

9.4.4 Uso de utilidades con privilegios del sistema

Control

Se debería restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

Guía de implantación

Deberían considerarse las siguientes directrices en el uso de programas de utilidades capaces de anular los controles del sistema y aplicación:

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

b) segregación de los programas de utilidades del software de aplicaciones;

c) limitar el uso de programas de utilidades al mínimo número viable de usuarios autorizados y de confianza (véase 9.2.3);

d) autorización para el uso ad-hoc de programas de utilidades;

e) limitar la disponibilidad de los programas de utilidades, por ejemplo, a la duración de un cambio autorizado;

f) registrar todo uso de programas de utilidades;

g) definir y documentar los niveles de autorización para los programas de utilidades;

h) eliminar o inhabilitar todos los programas de utilidades que no sean necesarios;

i) no poner los programas de utilidades a disposición de los usuarios con acceso a aplicaciones en los sistemas que requieran una segregación de funciones.

Información adicional

La mayoría de instalaciones de ordenadores poseen uno o más programas de utilidades capaces de anular los controles del sistema y de aplicación.

9.4.5 Control de acceso al código fuente de los programas

Control

Se debería restringir el acceso al código fuente de los programas.

Guía de implantación

El acceso al código fuente del programa y elementos relacionados (tales como diseños, especificaciones, planes de verificación y validación) deberían estar controlados estrictamente para prevenir la introducción de funcionalidades no autorizadas y para evitar cambios no intencionados, así como para mantener la confidencialidad de la propiedad intelectual de valor. Para el código fuente del programa, esto puede conseguirse controlando el almacenamiento centralizado del mismo, preferiblemente en librerías de programas fuente. Se deberían considerar las directrices siguientes para controlar el acceso a dichas librerías de programas fuentes y reducir el potencial de corrupción de los programas:

a) cuando sea posible, las librerías de programas fuente no deberían guardarse en los sistemas en producción o en explotación;

b) el código fuente del programa y las librerías de programas deberían gestionarse de acuerdo con los procedimientos establecidos;

c) el personal de soporte no debería tener acceso sin restricciones a las librerías de programas fuente;

d) la actualización de las librerías de programas fuente y elementos relacionados y su envío a los programadores debería ejecutarse sólo tras haber recibido la autorización adecuada;

e) los listados de programa deberían guardarse en un entorno seguro;

f) debería mantenerse un registro de auditoría de todos los accesos a las librerías de programas fuente;

g) el mantenimiento y copia de las librerías de programas fuente debería estar sujeto a procedimientos estrictos de control de cambios (véase 14.2.2).

Si se pretende publicar el código fuente, deberían considerarse controles adicionales para asegurar su integridad (por ejemplo, firmar electrónicamente).

10 Criptografía

10.1 Controles criptográficos

Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

10.1.1 Política de uso de los controles criptográficos

Control

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

Guía de implantación

Al desarrollar una política criptográfica, debería tenerse en cuenta lo siguiente:

a) el enfoque de la Dirección con respecto al uso de controles criptográficos en toda la organización, incluyendo los principios generales en base a los cuales debería protegerse la información de negocio;

b) tomando como base la evaluación de los riesgos, debería identificarse el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido;

c) el uso del cifrado para proteger la información sensible transportada a través de dispositivos móviles o extraíbles o a través de líneas de comunicación;

d) el enfoque de la gestión de las claves, incluyendo los métodos para ocuparse de la protección de las claves criptográficas y la recuperación de la información cifrada en caso de pérdida, vulneración o daño de las claves;

e) las funciones y responsabilidades; es decir, quién es responsable de:

   1) la implantación de la política,

   2) la gestión de las claves, incluyendo la generación de las mismas (véase 10.1.2),

f) las normas que deberían adoptarse para la implantación efectiva en toda la organización (qué solución se utilizará para cada proceso de negocio);

g) el impacto del uso de información cifrada en los controles que se basan en la inspección del contenido (por ejemplo, la detección de software malicioso (*malware*)).

Al implantar la política criptográfica de la organización, deberían tenerse en cuenta las regulaciones y restricciones nacionales que puedan resultar aplicables al uso de técnicas criptográficas en las distintas partes del mundo, así como a las cuestiones relativas al flujo transfronterizo de información cifrada (véase 18.1.5).

Los controles criptográficos pueden utilizarse para alcanzar distintos objetivos de seguridad, por ejemplo:

a) confidencialidad: uso del cifrado de la información para proteger información sensible o crítica, tanto si ésta se almacena como si se transmite;

b) integridad/autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para verificar la autenticidad o la integridad de la información sensible o crítica que se almacene o se transmita;

c) no repudio: uso de técnicas criptográficas para obtener pruebas de la existencia o inexistencia de un evento o una acción;

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

Información adicional

Tomar una decisión en cuanto a si una solución criptográfica resulta adecuada debería considerarse como parte del proceso general de evaluación de riesgos y selección de controles. En ese caso, esta evaluación podría utilizarse para determinar si un control criptográfico es adecuado, qué tipo de control debería aplicarse, para qué fin y en qué procesos de negocio.

La política sobre el uso de controles criptográficos resulta necesaria para maximizar los beneficios y minimizar los riesgos de utilizar técnicas criptográficas, así como para evitar un uso inadecuado o incorrecto.

Debería consultarse con un especialista al seleccionar los controles criptográficos que sean apropiados para cumplir con los objetivos de la política de seguridad de la información.

10.1.2 Gestión de claves

Control

Se debería desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

Guía de implantación

La política debería incluir los requisitos de gestión de las claves criptográficas en todo su ciclo de vida incluyendo la generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de las mismas.

Los algoritmos criptográficos, la extensión de las claves y las prácticas de uso deberían seleccionarse de acuerdo con buenas prácticas. Una gestión adecuada de las claves requiere procesos seguros de generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de las claves criptográficas.

Todas las claves criptográficas deberían estar protegidas contra la modificación, la pérdida y la destrucción de las mismas. Además, las claves secretas y privadas necesitan protección contra una revelación no autorizada de las mismas. Los equipos utilizados para generar, almacenar y archivar claves deberían contar con protección física.

El sistema de gestión de claves debería basarse en un conjunto consensuado de normas, procedimientos y métodos seguros para:

a) generar claves para distintos sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de clave pública;

c) distribuir las claves a los usuarios previstos, incluyendo la forma en que dichas claves deberían activarse cuando se reciban;

d) almacenar claves, incluyendo la forma en que los usuarios autorizados pueden acceder a las mismas;

e) cambiar o actualizar las claves, incluyendo las normas relativas a cuándo y cómo deberían cambiarse las claves;

f) actuar ante las claves comprometidas;

g) revocar claves, incluyendo cómo deberían retirarse o desactivarse las claves, por ejemplo, cuando éstas han sido comprometidas o cuando un usuario deja una organización (en cuyo caso, las claves también deberían archivarse);

h) recuperar claves perdidas o corruptas;

i) realizar copias de respaldo o archivar claves;

j) destruir claves;

k) registrar y auditar las actividades relacionadas con la gestión de las claves.

Para reducir la posibilidad de un uso inadecuado, deberían definirse fechas de activación y desactivación de las claves, de manera que éstas sólo puedan utilizarse durante un espacio limitado de tiempo definido en la correspondiente política de gestión de claves.

Además de una gestión segura de las claves secretas y privadas, también debería tenerse en cuenta la autenticidad de las claves públicas. Este proceso de autenticación puede llevarse a cabo utilizando certificados de clave pública, que suelen ser expedidos por una autoridad de certificación, que debería ser una organización reconocida que cuente con controles y procedimientos adecuados para ofrecer el grado de confianza necesario.

El contenido de los acuerdos o contratos de nivel de servicio con proveedores externos de servicios criptográficos como, por ejemplo, una autoridad de certificación, debería cubrir las cuestiones relativas a la responsabilidad, la fiabilidad de los servicios y los tiempos de respuesta para la prestación de servicios (véase 15.2).

Información adicional

La gestión de claves criptográficas resulta fundamental para un uso eficaz de las técnicas criptográficas. La Norma ISO/IEC 11770[2] [3] [4] ofrece más información acerca de la gestión de claves.

Las técnicas criptográficas pueden usarse asimismo para proteger las claves criptográficas. Puede que sea necesario considerar el uso de procedimientos para tratar los requisitos legales de acceso a las claves criptográficas; por ejemplo, puede que, en un juicio, deba presentarse información cifrada como prueba en un formato no cifrado.

11 Seguridad física y del entorno

11.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

11.1.1 Perímetro de seguridad física

Control

Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.

Guía de implantación

Se deberían considerar e implantar, cuando sea adecuado, las siguientes directrices para los perímetros de seguridad física:

a) los perímetros de seguridad deberían estar claramente definidos, y la situación y fortaleza de cada perímetro debería depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de la evaluación del riesgo;

b) los perímetros de un edificio o instalación que contiene los recursos de tratamiento de la información deberían ser físicamente sólidos (por ejemplo, no deberían existir huecos en el perímetro o áreas dónde pudieran producirse rupturas fácilmente); los tejados y muros externos y el solado del sitio deberían ser de construcción sólida y todas las puertas externas deberían estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo barras, alarmas, cerraduras, etc.; las puertas y ventanas deberían estar bloqueadas cuando no estén atendidas y se debería considerar una protección externa para las ventanas, en especial para las que se encuentran a nivel del suelo;

c) debería situarse un área de recepción atendida u otros controles de acceso físico a las instalaciones o al edificio; se deberían restringir los accesos a las instalaciones y edificios únicamente al personal autorizado;

d) las barreras físicas deberían, cuando sea aplicable, ser construidas para prevenir los accesos físicos no autorizados y la contaminación ambiental;

e) todas las puertas del perímetro de seguridad que actúen como cortafuegos deberían estar dotadas de un sistema de alarma, monitorizadas y probadas conjuntamente con las paredes, para establecer el nivel requerido de resistencia de acuerdo a las normas regionales, nacionales e internacionales; se debería operar de acuerdo a los códigos locales de protección contra incendios en modo de fallo seguro;

f) se deberían instalar sistemas de detección de intrusión adecuados conforme a las normas regionales, nacionales e internacionales y ser probados periódicamente para dar cobertura a todas las puertas externas y ventanas accesibles; las áreas no ocupadas deberían estar dotadas de un sistema de alarma en todo momento; se deberían también cubrir otras áreas, por ejemplo, la sala de ordenadores o las salas de comunicaciones;

g) los recursos de tratamiento de la información gestionados por la organización deberían estar físicamente separados de aquellos gestionados por terceras partes.

Información adicional

La protección física puede alcanzarse a través de la creación de una o más barreras físicas alrededor de las instalaciones de la organización y de los recursos de tratamiento de la información. El uso de barreras múltiples proporciona protección adicional, de manera que el fallo de una barrera en particular no significa que se comprometa inmediatamente la seguridad.

Un área segura puede ser una oficina que se pueda cerrar con llave o varias salas rodeadas por una barrera interna y continua de seguridad física. Pueden ser necesarias barreras adicionales y perímetros de control de acceso físico entre áreas dentro del perímetro de seguridad que tengan diferentes requisitos de seguridad. Se deberían proporcionar consideraciones especiales relativas a la seguridad de los accesos físicos, para edificios que albergan a diferentes organizaciones.

La aplicación de controles físicos, especialmente en las áreas seguras, debería ser adaptada a las circunstancias técnicas y económicas de la organización, según se establezca en la evaluación del riesgo.

11.1.2 Controles físicos de entrada

Control

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

Guía de implantación

Deberían considerarse las siguientes directrices:

a) se debería registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes deberían ser supervisados a menos que su acceso haya sido previamente aprobado; únicamente se debería conceder el acceso para propósitos específicos y autorizados, y junto con el acceso se deberían proporcionar las instrucciones de los requisitos de seguridad del área y los procedimientos de emergencia. La identidad de los visitantes debería autenticarse mediante los medios adecuados;

b) el acceso a las áreas dónde se procesa o se almacena información sensible debería estar controlado y restringido únicamente a personal autorizado; se deberían utilizar controles de autenticación para autorizar y validar todos los accesos, por ejemplo implantando un mecanismo de doble factor de autenticación como tarjetas de control de acceso con número de identificación personal secreto (PIN);

c) deberían mantenerse y monitorizarse de manera segura un libro físico de registro o una pista de auditoría electrónica de todos los accesos;

d) debería requerirse a todos los empleados, contratistas y terceros y a todos los visitantes, el llevar una identificación visible y debería notificarse inmediatamente al personal de seguridad si se encuentran visitantes sin acompañamiento o alguna persona sin llevar visible la identificación;

e) para el personal proveniente de terceros que prestan servicios de apoyo, se debería proporcionar acceso restringido a las áreas seguras o a los recursos de tratamiento de la información sensible únicamente cuando sea requerido; este acceso debería estar autorizado y controlado;

f) los derechos de acceso a las áreas seguras deberían ser revisados y actualizados regularmente, y revocados cuando sea necesario (véase 9.2.5 y 9.2.6).

11.1.3 Seguridad de oficinas, despachos y recursos

Control

Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.

Guía de implantación

Deberían considerarse las siguientes directrices para asegurar las oficinas, los despachos e instalaciones:

a) se deberían situar las instalaciones clave de manera que se evite el acceso por el público en general;

b) donde sea aplicable, los edificios deberían proporcionar de una manera discreta una mínima indicación de su función, con señales no obvias, que identifiquen la existencia de actividades de tratamiento de la información, ya sea fuera o dentro del edificio;

c) las instalaciones deberían configurarse para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior. Deberían considerarse los campos electromagnéticos si se considera adecuado;

d) los directorios y las guías telefónicas internas que identifiquen los emplazamientos de los recursos de tratamiento de la información sensible, no deberían ser de fácil acceso a la lectura por personas no autorizadas.

11.1.4 Protección contra las amenazas externas y ambientales

Control

Se debería diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

Guía de implantación

Se debería recabar asesoramiento especializado sobre cómo evitar daños causados por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.

11.1.5 El trabajo en áreas seguras

Control

Se deberían diseñar e implementar procedimientos para trabajar en las áreas seguras.

Guía de implantación

Deberían considerarse las siguientes directrices:

a) el personal debería conocer la existencia de un área segura, o de sus actividades, únicamente en el caso de que sea necesario para su trabajo;

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

c) las áreas seguras vacías deberían estar físicamente cerradas y ser comprobadas periódicamente;

d) no se deberían permitir equipos de fotografía, video, audio u otros equipos de grabación, salvo autorización especial;

Las disposiciones para trabajar en áreas seguras incluyen los controles para los empleados, contratistas y terceros que trabajan en el área segura, así como para otras actividades de terceros que tengan lugar allí.

11.1.6 Áreas de carga y descarga

Control

Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

Guía de implantación

Se deberían considerar las siguientes directrices:

a) se deberían restringir los accesos a las áreas de carga y descarga desde el exterior sólo para el personal autorizado e identificado;

b) el área de carga y descarga se debería diseñar de tal manera que los suministros puedan cargarse y descargarse sin que el personal de entrega tenga que acceder a otras zonas del edificio;

c) la puertas externas de un área de carga y descarga deberían estar cerradas cuando las puertas internas estén abiertas;

d) el material entrante debería ser inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo antes de trasladarlo desde el área de carga y descarga hasta su lugar de utilización;

e) el material entrante debería registrarse de acuerdo a los procedimientos de gestión de activos (véase el capítulo 8) al entrar en la instalación;

f) cuando sea posible, se debería separar físicamente la entrada y la salida de envíos;

g) el material entrante debería inspeccionarse en busca de indicios de manipulación durante su traslado. Si se descubre tal manipulación se debería informar de inmediato al personal de seguridad.

11.2 Seguridad de los equipos

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

11.2.1 Emplazamiento y protección de equipos

Control

Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.

Guía de implantación

Se deberían considerar las siguientes directrices para proteger los equipos:

a) los equipos deberían situarse de tal manera que se minimicen los accesos innecesarios a las áreas de trabajo;

b) los equipos de tratamiento de información que manejen datos sensibles se deberían instalar donde se reduzca el riesgo de que la información sea vista durante su uso por personas no autorizadas;

c) las instalaciones de almacenamiento deberían asegurarse para evitar los accesos no autorizados;

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

e) se deberían adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua (o fallo de suministro de agua), polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo;

f) deberían establecerse directrices para comer, beber y fumar en las proximidades de las instalaciones de tratamiento de información;

g) se deberían controlar las condiciones ambientales, tales como la temperatura y la humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información;

h) se deberían aplicar sistemas de protección contra rayos en todos los edificios y colocar filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación;

i) se debería considerar el uso de métodos de protección especial, por ejemplo cubiertas para teclados, en el caso de los equipos situados en entornos industriales;

j) se deberían proteger los equipos que procesen la información sensible para minimizar el riesgo de fugas de información debidas a una emanación electromagnética.

11.2.2 Instalaciones de suministro

Control

Los equipos deberían estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

Guía de implantación

Los suministros de apoyo como, por ejemplo, electricidad, telecomunicaciones, agua, gas, aguas residuales, calefacción/ventilación y aire acondicionado, deberían:

a) ser conformes a las especificaciones del fabricante de los equipos y a los requisitos legales locales;

b) ser evaluadas regularmente respecto a su capacidad para satisfacer el desarrollo de negocio y respecto a la interacción con otros servicios de apoyo;

c) ser inspeccionadas regularmente mediante las pruebas apropiadas para asegurar su correcto funcionamiento;

d) en caso necesario, disponer de alarmas para detectar fallos en su funcionamiento;

e) en caso necesario, disponer de múltiples fuentes con canales físicos de alimentación independientes.

Debería proporcionarse alumbrado y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otros servicios no deberían estar ubicados cerca de las salidas de emergencia o de las salas de los equipos.

Información adicional

Se puede conseguir redundancia adicional para la conectividad de las redes por medio de múltiples rutas aportadas por más de un proveedor de servicios.

11.2.3 Seguridad del cableado

Control

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

Guía de implantación

Se deberían considerar las siguientes directrices para la seguridad del cableado:

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

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

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

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

    2) uso de apantallamiento electromagnético para proteger los cables,

    3) implantación de barreras técnicas e inspecciones físicas para detectar la conexión al cableado de dispositivos no autorizados,

    4) accesos controlados a los paneles de parcheo y a las salas de cableado.

11.2.4 Mantenimiento de los equipos

Control

Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

Guía de implantación

Se deberían considerar las siguientes directrices para el mantenimiento de los equipos:

a) los equipos deberían mantenerse de acuerdo a las recomendaciones de intervalos de servicio y especificaciones del proveedor;

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

c) se deberían mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo;

d) se deberían adoptar los controles adecuados cuando se programen los equipos para su mantenimiento, teniendo en cuenta si el mantenimiento se lleva a cabo por personal en la propia organización o en un lugar externo; cuando sea necesario, la información sensible debería ser borrada del equipo;

e) se debería cumplir con todos los requisitos de mantenimiento que exijan las pólizas de seguros;

f) antes de poner el equipo de nuevo en funcionamiento después de su mantenimiento, debería ser inspeccionado para asegurar que el equipo no ha sido manipulado y que no funciona incorrectamente.

11.2.5 Retirada de materiales propiedad de la empresa

Control

Sin autorización previa, los equipos, la información o el software no deberían sacarse de las instalaciones.

Guía de implantación

Se deberían considerar las siguientes directrices:

a) los empleados y usuarios de terceras partes con permiso para sacar los activos fuera de las instalaciones, deberían estar claramente identificados;

b) se deberían establecer limitaciones al tiempo que el equipo puede estar fuera de las instalaciones y verificar a su retorno que se ha cumplido con dichas limitaciones;

c) dónde sea necesario y adecuado, se debería registrar la salida de equipos fuera de los locales de la organización, así como su retorno;

d) la identidad, las funciones y la afiliación de cualquier persona que maneja o usa los activos deberían documentarse y esta documentación regresar juntamente con el equipo, información o software.

Información adicional

También se pueden realizar inspecciones al azar llevadas a cabo para detectar salidas de activos no autorizadas, dispositivos de grabación no autorizados, armas, etc. y para prevenir su introducción en las instalaciones. Tales inspecciones al azar deberían llevarse a cabo de acuerdo con la legislación y normativa aplicable. Los individuos deberían tener conocimiento de que se están llevando a cabo tales inspecciones al azar, y las comprobaciones deberían realizarse únicamente con la adecuada autorización conforme con los requisitos legales y reglamentarios.

11.2.6 Seguridad de los equipos fuera de las instalaciones

Control

Deberían aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

Guía de implantación

Todo uso fuera de las instalaciones de la organización de cualquier equipo que almacene o trate información debería ser autorizado por la dirección. Esto aplica a los equipos propiedad de la organización y a los equipos propiedad del usuario pero utilizado en nombre de la organización.

Se deberían considerar las siguientes directrices para la protección de los equipos fuera de las instalaciones de la organización:

a) los equipos y soportes sacados de las instalaciones no se deberían dejar desatendidos en lugares públicos;

b) se deberían respetar en todo momento las instrucciones del fabricante relativas a la protección de los equipos, por ejemplo, sobre la protección contra exposiciones a campos electromagnéticos intensos;

c) se deberían determinar los controles para emplazamientos fuera de las instalaciones de la organización incluyendo el trabajo en el domicilio personal, teletrabajo y lugares de trabajo temporales, mediante una evaluación del riesgo y, cuando corresponda, aplicarse los controles convenientes, por ejemplo, archivadores que se puedan cerrar, una política de puesto de trabajo despejado, controles de acceso a los ordenadores y comunicación segura con la oficina (véase también la Norma ISO/IEC 27033 [15][16][17][18][19]);

d) cuando el equipo fuera de las instalaciones se transfiere entre diferentes individuos o entidades externas, se debería mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las organizaciones de aquellos responsables de los equipos.

Los riesgos de seguridad, por ejemplo, de daño, robo o escucha, pueden variar considerablemente según la ubicación y deberían tenerse en cuenta al determinar los controles que sean más adecuados.

Información adicional

Los equipos de tratamiento y de almacenamiento de la información comprenden todo tipo de ordenadores personales, organizadores, teléfonos móviles, tarjetas inteligentes, documentos en formato papel o en otros formatos, que se lleven al domicilio personal o fuera del lugar habitual de trabajo.

Más información sobre otros aspectos de protección de los equipos móviles puede encontrarse en 6.2.

Puede ser apropiado para evitar riesgos, desalentar a ciertos empleados de trabajar fuera de las instalaciones o restringirles el uso de los equipos de TI portátiles.

11.2.7 Reutilización o eliminación segura de equipos

Control

Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

Guía de implantación

Debería comprobarse si los equipos contienen medios de almacenamiento o no antes de su retirada o reutilización.

Los soportes que contengan información sensible o con derechos de autor deberían ser destruidos físicamente o bien la información debería ser destruida, borrada o sobrescrita mediante técnicas que hagan imposible la recuperación de la información original, en lugar de utilizar un borrado o un formateado normal.

Información adicional

Los dispositivos de almacenamiento dañados que contengan datos sensibles pueden requerir una evaluación del riesgo para determinar si deberían ser destruidos físicamente en lugar de repararse o eliminarse. La información puede verse comprometida por una eliminación o reutilización no cuidadosa de los equipos.

Adicionalmente al borrado seguro de los discos, un cifrado completo de los mismos reduce el riesgo de divulgación de la información confidencial cuando el equipo es retirado o, en el caso de ser redistribuido, siempre que:

a) el proceso de cifrado sea suficientemente fuerte y cubra el disco completamente (incluyendo el espacio libre, archivos temporales de intercambio de memoria, etc.);

b) las contraseñas de cifrado son suficientemente largas para resistir ataques de fuerza bruta;

c) las contraseñas de cifrado se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para consejos adicionales sobre cifrado, véase el capítulo 10.

Las técnicas para una sobrescritura segura de los dispositivos de almacenamiento pueden diferir en función de la tecnología. Las herramientas de sobrescritura deberían ser revisadas para asegurar que son aplicables a la tecnología de los dispositivos de almacenamiento.

11.2.8 Equipo de usuario desatendido

Control

Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.

Guía de implantación

Todos los usuarios deberían ser conscientes de los requisitos y los procedimientos de seguridad para proteger el equipo desatendido, así como de sus responsabilidades para la implantación de dicha protección. Los usuarios deberían ser asesorados para:

a) terminar las sesiones activas cuando se acaben, a menos que estén aseguradas a través de un mecanismo de bloqueo adecuado, por ejemplo, protector de pantalla con contraseña;

b) salir de las aplicaciones o servicios de red cuando ya no se necesiten;

c) asegurar los ordenadores personales o los terminales frente a accesos no autorizados a través de un bloqueo con clave o un control equivalente, por ejemplo, contraseñas de acceso cuando no están en uso.

11.2.9 Política de puesto de trabajo despejado y pantalla limpia

Control

Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

Guía de implantación

La política de puesto de trabajo despejado y pantalla limpia debería tener en cuenta las clasificaciones de la información (véase 8.2), los requisitos legales y contractuales (véase 18.1), y los correspondientes riesgos y aspectos culturales de la organización. Se deberían considerar las siguientes directrices:

a) la información de negocio sensible o crítica, por ejemplo, en papel o en soportes de almacenamiento electrónico, debería estar guardada (idealmente en una caja fuerte, armario u otro tipo de mueble de seguridad), cuando no se necesite, especialmente cuando la oficina esté vacía;

b) los ordenadores y terminales deberían quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, dispositivo hardware o mecanismo similar de autenticación de usuario cuando estén desatendidos y deberían estar protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso;

c) debería prevenirse el uso por usuarios no autorizados de fotocopias y otros dispositivos de reproducción (por ejemplo, escáneres, cámaras digitales);

d) los soportes que contengan información sensible o clasificada deberían retirarse de manera inmediata de las impresoras.

Información adicional

Una política de puesto de trabajo despejado y pantalla limpia reduce los riesgos de accesos no autorizados, pérdida o daño de la información tanto durante las horas normales de trabajo como fuera de ellas. Las cajas fuertes u otras formas de almacenamiento seguro pueden proteger la información almacenada también contra desastres tales como el fuego, un terremoto, una inundación o una explosión.

Considerar el uso de impresoras con función de código PIN, de esta manera los autores son los únicos que pueden obtener sus impresiones, y además hacerlo únicamente cuando estén delante de la impresora.

12 Seguridad de las operaciones

12.1 Procedimientos y responsabilidades operacionales

Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

12.1.1 Documentación de procedimientos de los operación

Control

Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

Guía de implantación

Se deberían preparar procedimientos documentados para las actividades del sistema asociadas a los recursos de tratamiento y comunicación de la información, tales como procedimientos de encendido y apagado de ordenadores, copias de respaldo, mantenimiento de los equipos, gestión de soportes, gestión de salas de ordenadores, gestión del correo, y seguridad.

Los procedimientos operativos deberían especificar las instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) la instalación y configuración de sistemas;

b) el tratamiento y manipulación de la información tanto automatizada como manual;

c) las copias de respaldo (véase 12.3);

d) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos más tempranos de comienzo y más tardíos de finalización posibles de cada tarea;

e) las instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la ejecución del trabajo, incluyendo restricciones en el uso de las utilidades del sistema (véase 9.4.4.);

f) los contactos de soporte y escalado, incluyendo contactos de soporte externo, para el caso de dificultades operacionales o técnicas inesperadas;

g) las instrucciones para el manejo de resultados especiales y soportes, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de destrucción segura de resultados producidos como consecuencia de tareas fallidas (véanse 8.3 y 11.2.7);

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

i) la gestión de pistas de auditoría y de la información del registro de sistemas (véase 12.4);

j) los procedimientos de monitorización.

Los procedimientos operacionales, y los procedimientos documentados para las actividades del sistema deberían tratarse como documentos formales y los cambios deberían ser autorizados por la dirección. Dónde sea técnicamente posible, los sistemas de información deberían gestionarse de una manera sistemática, utilizando los mismos procedimientos, herramientas y recursos.

12.1.2 Gestión de cambios

Control

Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.

Guía de implantación

En particular, se deberían considerar los siguientes puntos:

a) la identificación y registro de los cambios significativos;

b) la planificación y pruebas de los cambios;

c) la evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información de dichos cambios;

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

e) la verificación de que los requisitos de seguridad de la información se cumplen;

f) la comunicación de los detalles de los cambios a todas las personas correspondientes;

g) los procedimientos de vuelta atrás, incluyendo los procedimientos y responsabilidades para abortar y recuperar los cambios infructuosos y los eventos imprevistos;

h) la disposición de un proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente (véase 16.1).

Los procedimientos y las responsabilidades formales de gestión deberían asegurar de una manera satisfactoria el control de todos los cambios. Cuando se efectúen los cambios, se debería conservar un registro de auditoría que contenga toda la información importante.

Información adicional

El control inadecuado de los cambios en los recursos y en los sistemas de tratamiento de la información es una causa común de fallos de seguridad de los sistemas. Los cambios en el entorno operativo pueden impactar en la fiabilidad de las aplicaciones, especialmente cuando se transfiere un sistema desde la fase de desarrollo a la de operación (véase 14.2.2).

12.1.3 Gestión de capacidades

Control

Se debería supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

Guía de implantación

Se deberían identificar los requisitos de capacidad, teniendo en cuenta el carácter crítico para el negocio del sistema en cuestión. Se deberían aplicar sistemas de control y de ajuste para asegurar, donde sea necesario, la mejora de la disponibilidad y de la eficiencia de los sistemas. Se deberían implantar controles de detección para identificar la existencia de problemas a su debido tiempo. Las proyecciones de requisitos futuros de capacidad deberían tener en cuenta nuevas líneas de negocio y nuevos sistemas, así como las tendencias actuales y las previstas para las capacidades de tratamiento de la información de la organización.

Es necesario poner una atención especial en aquellos recursos que tengan un periodo de adquisición o plazos de entrega largos o sean de coste elevados; por consiguiente, los gerentes o responsables deberían supervisar la utilización de los recursos claves del sistema. Deberían identificar las tendencias de uso, particularmente en lo que respecta a las aplicaciones de negocio o a las herramientas del sistema de gestión de la información.

Los directivos o responsables deberían utilizar esta información para identificar y evitar posibles cuellos de botella o dependencias de personal clave que pudieran representar una amenaza para el sistema de seguridad o para los servicios y planificar las acciones adecuadas.

Se puede proporcionar suficiente capacidad mediante el incremento de la misma o reduciendo la demanda. Ejemplos de gestión de la demanda de capacidad incluyen:

a) borrado de datos obsoletos (espacio de disco);

b) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos;

c) optimizando el tratamiento por lotes y la planificación;

d) optimizando la lógica de la aplicación o las consultas de base de datos;

e) denegando o restringiendo el ancho de banda para servicios consumidores de muchos recursos, si estos no son críticos para el negocio (por ejemplo, la transmisión de vídeo).

Se debería considerar un plan documentado de gestión de la capacidad para los sistemas de misión crítica.

Información adicional

Este control cubre también la capacidad de los recursos humanos, así como oficinas e instalaciones.

12.1.4 Separación de los recursos de desarrollo, prueba y operación

Control

Deberían separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

Guía de implantación

Se debería identificar e implantar el nivel de segregación entre los entornos de operación, de prueba y de desarrollo que sea necesario para prevenir problemas operacionales.

Se deberían considerar los siguientes puntos:

a) definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hasta el estado de operación;

b) el software de desarrollo y explotación debería ejecutarse en diferentes sistemas o procesadores de ordenador y en diferentes dominios o directorios;

c) los cambios en las aplicaciones y sistemas en operación deberían probarse en un entorno de pruebas o ensayo de modo previo a ser aplicados en sistemas en operación;

d) salvo en circunstancias excepcionales, las pruebas no se deberían hacer en los sistemas en operación;

e) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas de operación cuando no sea necesario;

f) los usuarios deberían utilizar diferentes perfiles para los sistemas de operación y de prueba, y los menús deberían mostrar mensajes de identificación adecuados para reducir el riesgo de error;

g) los datos sensibles no deberían ser copiados en el entorno del sistema de prueba, a menos que se proporcionen controles equivalentes en dicho entorno (véase 14.3).

Información adicional

Las actividades de desarrollo y de prueba pueden causar problemas serios, por ejemplo, la modificación no deseada de ficheros o del entorno del sistema, o fallo del sistema. En este caso, es necesario mantener un entorno conocido y estable para llevar a cabo pruebas determinantes, así como para prevenir el acceso inapropiado de los desarrolladores al entorno de producción.

Cuando el personal de desarrollo y de prueba tiene acceso al sistema de producción y a su información, pueden introducir código no autorizado y que no ha sido probado o datos operativos modificados. En algunos sistemas, esta capacidad podría utilizarse para cometer fraude o para introducir un código malicioso o no probado, que puede causar problemas operacionales serios.

El personal de desarrollo y de prueba puede suponer también una amenaza para la confidencialidad de la información. Si las actividades de desarrollo y de prueba comparten el mismo entorno informático puede causar cambios no intencionados en el software o en la información. La separación de los entornos de desarrollo, prueba y de producción es, por tanto, deseable para reducir el riesgo de cambios accidentales o accesos no autorizados al software de producción y a los datos de negocio (véase 14.3 en lo relativo a la protección de los datos de prueba).

12.2 Protección contra el software malicioso (*malware*)

Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el *malware*.

12.2.1 Controles contra el código malicioso

Control

Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

Guía de implantación

La protección contra el código malicioso debería estar basada en un software de detección de código malicioso y de reparación, la concienciación en seguridad, y los controles adecuados para el acceso a los sistemas y para la gestión del cambio. Se deberían considerar las siguientes directrices:

a) el establecimiento de una política formal prohibiendo el uso de software no autorizado (véase 12.6.2 y 14.2);

b) la implantación de controles que prevengan o detecten el uso de software no autorizado (por ejemplo, una lista de aplicaciones autorizadas);

c) la implantación de controles para prevenir o detectar el uso de sitios web de los que se conoce o sospecha su carácter malicioso (por ejemplo, listas negras);

d) el establecimiento de una política formal para proteger contra los riesgos asociados a la obtención de ficheros y software, ya sea a través de redes externas, o de cualquier otro medio, indicando las medidas de protección que deberían tomarse;

e) la reducción de vulnerabilidades que podrían ser explotadas por el código malicioso, por ejemplo, a través de una gestión de vulnerabilidades técnicas (véase 12.6);

f) llevar a cabo revisiones regulares del software y datos contenidos en los sistemas que soportan los procesos críticos del negocio; la presencia de cualquier fichero no aprobado o modificación no autorizada debería ser formalmente investigada;

g) la instalación y actualización regular de software de detección y reparación de código malicioso para escanear los ordenadores y los dispositivos, como control preventivo o rutinario; las comprobaciones llevadas a cabo deberían incluir:

   1) la comprobación frente a código malicioso antes de su uso, de cualquier fichero recibido a través de redes, o vía cualquier forma de soporte, electrónico u óptico,

   2) la comprobación frente a código malicioso antes de su uso, de los adjuntos al correo electrónico y las descargas; esta comprobación debería llevarse a cabo en diferentes lugares, por ejemplo, en los servidores de correo electrónico, los ordenadores de sobremesa y en la entrada de las redes de la organización,

   3) la comprobación de páginas web para detectar código malicioso,

h) definir procedimientos y responsabilidades de gestión para tratar la protección de los sistemas contra el código malicioso, la formación en su uso, así como en el informe y recuperación de los ataques de código malicioso;

i) preparar planes adecuados de continuidad de negocio para la recuperación de los ataques de código malicioso, incluyendo todos los datos y software de respaldo y disposiciones de recuperación necesarios (véase 12.3);

j) implantar procedimientos para recogida de información de manera regular, tales como suscripción a listas de correo o revisión de páginas web que contengan información sobre nuevos códigos maliciosos;

k) implantar procedimientos para verificar la información relativa al código malicioso, y asegurar que los boletines de alerta son precisos e informativos; los gerentes deberían asegurarse de que se están utilizando fuentes de confianza, tales como publicaciones acreditadas, sitios de Internet o suministradores que producen software de protección contra código malicioso fiables, para diferenciar entre correos electrónicos engañosos (*hoaxes*) y código malicioso real; todos los usuarios deberían ser conscientes del problema de los correos electrónicos engañosos (*hoaxes*) y qué hacer cuando se reciban;

l) aislar los entornos cuando puedan producirse impactos catastróficos.

Información adicional

El uso de dos o más productos de software de protección contra código malicioso proveniente de diferentes suministradores puede mejorar la eficacia de la protección contra el código malicioso.

Debería tenerse cuidado para proteger contra la entrada de código malicioso durante los procedimientos de mantenimiento y de emergencia, durante los que pueden evitarse los controles normales de protección contra el código malicioso.

Bajo determinadas condiciones, la protección contra código malicioso puede ocasionar perturbaciones en las operaciones.

El uso de software de detección y reparación de código malicioso solo como control de código malicioso no es por lo general adecuado y necesita acompañarse de procedimientos de operaciones que prevengan la introducción de código malicioso.

12.3 Copias de seguridad

Objetivo: Evitar la pérdida de datos.

12.3.1 Copias de seguridad de la información

Control

Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

Guía de implantación

Debería establecerse una política de respaldo que defina los requisitos para las copias de respaldo de la información, el software y los sistemas.

La política de respaldo debería definir los requisitos de conservación y protección.

Deberían proporcionarse los recursos adecuados para las copias de respaldo para asegurar que toda la información y software esenciales pueden ser recuperados después de un desastre o fallo de los soportes.

Cuando se diseña un plan de respaldo, deberían considerarse los siguientes aspectos:

a) se deberían producir registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados;

b) la extensión (por ejemplo, copias totales o diferenciales) y frecuencia de las copias de respaldo deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información implicada y la criticidad de la información para el funcionamiento continuo de la organización;

c) las copias de respaldo deberían ser almacenadas en un emplazamiento alejado, a una distancia suficiente para salvarse de cualquier daño proveniente de un desastre en el emplazamiento principal;

d) la información de las copias de respaldo debería tener un nivel adecuado de protección tanto física como ambiental (véase el capítulo 11), consistente con las normas aplicadas en el emplazamiento principal;

e) los soportes de las copias de respaldo deberían ser comprobados periódicamente para asegurarse de que pueden responder en caso de uso de emergencia cuando sea necesario; esto debería combinarse, periódicamente, con una comprobación del funcionamiento de los procedimientos de recuperación y una prueba para asegurar que son efectivos y que pueden ser cumplidos dentro del tiempo asignado en los procedimientos operacionales para recuperación. Poner a prueba la capacidad para restaurar la copia de respaldo debería realizarse sobre los medios de prueba dedicados, y no sobrescribiendo los soportes originales, por si fallase el proceso de copiado o restauración y causara un daño o pérdida irreparable de datos;

f) en las situaciones donde es importante la confidencialidad, las copias de respaldo deberían ser protegidas mediante cifrado.

Los procedimientos operacionales deberían supervisar la ejecución de copias de respaldo e identificar los fallos de realización de copias de respaldo programadas para garantizar la integridad de las copias de respaldo, de acuerdo con la política de respaldo.

Las disposiciones de copias de respaldo para los sistemas individuales deberían ser regularmente probadas para asegurarse de que son conformes a los requisitos de los planes de continuidad de negocio. Para los sistemas críticos, las disposiciones de copias de respaldo deberían cubrir todos los sistemas de información, así como las aplicaciones y los datos necesarios para la recuperación del sistema completo en caso de desastre.

Debería determinarse el periodo de conservación para la información esencial del negocio, teniendo en cuenta cualquier requisito para las copias de archivo que hayan de ser conservadas de manera permanente.

12.4 Registros y supervisión

Objetivo: Registrar eventos y generar evidencias.

12.4.1 Registro de eventos

Control

Se deberían registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Guía de implantación

Los registros de eventos deberían incluir, cuando sea relevante:

a) identificadores (ID) de usuario;

b) actividades del sistema;

c) fechas, tiempos y detalles de eventos clave, por ejemplo, conexión (*log-on*) y desconexión (*log-off*);

d) identidad o localización del dispositivo, si es posible e identidad del sistema;

e) registro de intentos de acceso a los sistemas exitosos y fallidos;

f) registro de intentos de acceso a los recursos y a los datos exitosos y fallidos;

g) cambios en la configuración del sistema;

h) uso de privilegios;

i) uso de utilidades y aplicaciones del sistema;

j) ficheros a los que se ha accedido y el tipo de acceso;

k) direcciones y protocolos de red;

l) alarmas generadas por el sistema de control de acceso;

m) activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión;

n) registro de transacciones ejecutadas por usuarios en las aplicaciones.

El registro de eventos establece las bases para los sistemas automatizados de supervisión que son capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

Información adicional

Los registros de eventos pueden contener datos sensibles y datos personales. Se deberían tomar las medidas adecuadas de protección de la privacidad (véase 18.1.4).

Dónde sea posible, los administradores del sistema no deberían tener permiso para borrar o desactivar los registros de sus propias actividades (véase 12.4.3).

12.4.2 Protección de la información del registro

Control

Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.

Guía de implantación

Los controles deberían dirigirse a proteger contra los cambios no autorizados y los problemas operacionales relativos a los dispositivos e información de registro, incluyendo:

a) alteraciones en los tipos de mensajes que son registrados;

b) edición o borrado de los ficheros de registro;

c) superación de la capacidad de almacenamiento de los soportes de ficheros de registro, provocando bien un fallo del registro de eventos o bien sobrescribiendo los registros de eventos pasados.

Algunos registros de auditoría pueden requerir ser archivados como parte de la política de conservación de registros o debido a requisitos para recopilar y conservar evidencias (véase 16.1.7).

Información adicional

Los registros del sistema a menudo contienen un gran volumen de información, mucha de la cual no tiene relación con la monitorización de la seguridad. Se deberían considerar, para ayudar a la identificación de las incidencias significativas para los fines de monitorización de la seguridad, el copiado de manera automática de los tipos de mensajes apropiados a un segundo registro o el uso de los recursos adecuados del sistema o de herramientas de auditoría para realizar la consulta y la racionalización del fichero.

Los registros del sistema necesitan estar protegidos, porque si los datos que contienen pueden modificarse o borrarse, su existencia puede crear una falsa sensación de seguridad. El copiado en tiempo real de los registros en un sistema fuera del control del administrador u operador del sistema puede servir para salvaguardar los registros.

12.4.3 Registros de administración y operación

Control

Se deberían registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.

Guía de implantación

Los titulares de cuentas de usuario con privilegios pueden ser capaces de manipular los registros en las instalaciones de tratamiento de información bajo su control directo, por lo que es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios con privilegios.

Información adicional

Un sistema de detección de intrusos administrado fuera del control de los administradores del sistema y de la red se puede utilizar para supervisar las actividades del sistema y el cumplimiento de las actividades de administración de la red.

12.4.4 Sincronización del reloj

Control

Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deberían estar sincronizados con una única fuente de tiempo precisa y acordada.

Guía de implantación

Se deberían documentar los requisitos externos e internos para la representación, sincronización y precisión del tiempo. Tales requisitos pueden ser legales, reglamentarios, contractuales, de cumplimiento de normas o requisitos de supervisión interna. Debería establecerse para su uso dentro de la organización un tiempo de referencia normalizado.

Debería documentarse e implantarse el enfoque de la organización para obtener un tiempo de referencia de una fuente(s) externa así como la forma de sincronizar los relojes internos.

Información adicional

La correcta configuración de los relojes de los equipos es importante para garantizar la precisión de los registros de auditoría, que pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios. Unos registros de auditoría imprecisos pueden obstaculizar tales investigaciones y dañar la credibilidad de dicha evidencia. Un reloj enlazado con la radiodifusión de información horaria desde un reloj nacional atómico puede utilizarse como reloj maestro para los sistemas de registro. Un protocolo de red de tiempo puede ser usado para mantener todos los servidores sincronizados con el reloj maestro.

12.5 Control del software en explotación

Objetivo: Asegurar la integridad del software en explotación.

12.5.1 Instalación del software en explotación

Control

Se deberían implementar procedimientos para controlar la instalación del software en explotación.

Guía de implantación

Deberían tenerse en cuenta las siguientes directrices con el fin de controlar los cambios de software en los sistemas en explotación:

a) la actualización del software operacional, de las aplicaciones y de las bibliotecas de programas sólo debería ser llevada a cabo por administradores formados con la adecuada autorización de la dirección (véase 9.4.5);

b) los sistemas operativos sólo deberían manejar códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

c) el software de las aplicaciones y del sistema operativo sólo debería implantarse tras haber superado exhaustivas pruebas, que deberían incluir pruebas de usabilidad, seguridad, efectos en otros sistemas y facilidad de uso y deberían llevarse a cabo en sistemas independientes (véase 12.1.4); debería asegurarse que todas las bibliotecas fuente del programa correspondiente han sido actualizadas;

d) debería emplearse un sistema de control de la configuración para supervisar todo el software implantado, así como la documentación del sistema;

e) debería existir una estrategia de vuelta atrás antes de implantar los cambios;

f) debería mantenerse un registro de auditoría de todas las actualizaciones de las bibliotecas de los programas en explotación;

g) deberían conservarse versiones anteriores del software de las aplicaciones como medida de contingencia;

h) deberían archivarse las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de apoyo durante todo el tiempo en que la información se conserve en el archivo.

El software adquirido a proveedores que se utilice en los sistemas en explotación debería mantenerse en un nivel que cuente con la asistencia técnica del proveedor. Con el tiempo, los proveedores de software ya no ofrecerán asistencia para las versiones antiguas del software. La organización debería considerar los riesgos de utilizar software sin contar con asistencia técnica.

La decisión de pasar a una nueva versión debería tener en cuenta los requisitos de negocio para los cambios y la seguridad de la versión; es decir, la introducción de nuevas funciones de seguridad o el número y la gravedad de los problemas de seguridad que afecten a esta versión. Deberían aplicarse parches de software cuando éstos puedan ayudar a eliminar o a reducir los puntos débiles de seguridad (véase 12.6).

Sólo debería concederse acceso físico o lógico a los proveedores para que presten servicios de asistencia técnica cuando sea necesario y con una autorización por parte de la dirección. Las actividades del proveedor deberían supervisarse (véase 15.2.1).

El software informático puede depender de software y de módulos adquiridos externamente, que deberían ser supervisados y controlados para evitar cambios no autorizados, ya que éstos podrían generar un punto débil de seguridad.

12.6 Gestión de la vulnerabilidad técnica

Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas

Control

Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

Guía de implantación

Un requisito previo para la gestión efectiva de las vulnerabilidades técnicas es la elaboración de un inventario actual y completo de los activos (véase el capítulo 8). La información específica que se requiere para dar soporte a la gestión de vulnerabilidades técnicas incluye el proveedor de software, los números de versión, el estado actual de implantación (por ejemplo, qué software está instalado en qué sistemas) y la persona o personas de la organización responsables del software.

Deberían adoptarse medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas. Deberían seguirse las siguientes directrices con el fin de establecer un proceso efectivo de gestión de las vulnerabilidades técnicas:

a) la organización debería definir y establecer las funciones y responsabilidades asociadas con la gestión de las vulnerabilidades técnicas, incluyendo la supervisión de vulnerabilidades, la evaluación de riesgos de la vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria;

b) deberían identificarse los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la alerta sobre ellas, tanto para el software como para otras tecnologías (en función del inventario de activos, véase 8.1.1); estos recursos de información deberían actualizarse según se modifique el inventario o cuando se encuentren otros recursos nuevos o que sean de utilidad;

c) debería definirse una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que puedan resultar relevantes;

d) una vez identificada la vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las medidas que deberían adoptarse, las cuales podrían incluir el parcheo de sistemas vulnerables o la aplicación de otros controles;

e) dependiendo de la urgencia con que deba tratarse la vulnerabilidad técnica, la medida adoptada debería ser llevada a cabo de acuerdo con los controles relativos a la gestión de cambios (véase 12.1.2) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (véase 16.1.5);

f) si existe un parche disponible de una fuente legítima, deberían evaluarse los riesgos asociados con la instalación del mismo (deberían compararse los riesgos planteados por la vulnerabilidad con los riesgos de instalar el parche);

g) los parches deberían ser probados y evaluados antes de su instalación para garantizar que son efectivos y que no tienen efectos secundarios que no puedan ser aceptados. Si no hay ningún parche disponible, deberían considerarse otros controles, como:

    1) la desactivación de servicios o capacidades relacionadas con la vulnerabilidad,

    2) la adaptación o la inclusión de controles de acceso, como por ejemplo, cortafuegos, en los límites de la red (véase 13.1),

    3) el incremento de la supervisión para detectar o evitar ataques reales,

    4) el aumento de la concienciación sobre la vulnerabilidad,

h) debería mantenerse un registro de auditoría de todos los procedimientos adoptados;

i) el proceso de gestión de las vulnerabilidades técnicas debería supervisarse y evaluarse periódicamente para garantizar su efectividad y su eficacia;

j) los sistemas con elevado riesgo deberían ser los primeros en tratarse;

k) un proceso eficaz de gestión de las vulnerabilidades técnicas debería estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre las vulnerabilidades relativas a la función de respuesta a incidentes y proporcionar procedimientos técnicos a desarrollar cuando ocurra un incidente;

l) definir un procedimiento para considerar la situación donde una vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida. En esta situación, la organización debería evaluar los riesgos relativos a la vulnerabilidad conocida y definir acciones de detección y corrección adecuadas.

Información adicional

La gestión de vulnerabilidades técnicas puede considerarse una función secundaria de la gestión de cambios y, como tal, puede beneficiarse de los procesos y procedimientos de la misma (véanse 12.1.2 y 14.2.2).

Los proveedores suelen estar sometidos a mucha presión para publicar parches lo antes posible. Por ello, un parche puede no cubrir el problema correctamente y tener efectos secundarios negativos. Asimismo, en algunos casos, puede que no sea fácil desinstalar un parche una vez que se ha aplicado.

Si no es posible probar de manera adecuada los parches, por ejemplo, por motivos de coste o por falta de recursos, puede considerarse la opción de retrasar el parcheo para evaluar los riesgos asociados en función de la experiencia de otros usuarios. El uso de la Norma ISO/IEC 27031[14] puede ser beneficioso.

12.6.2 Restricción en la instalación de software

Control

Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

Guía de implantación

La organización debería definir y hacer cumplir una estricta política sobre qué tipos de software pueden instalar los usuarios.

Debería aplicarse el principio de menor privilegio. Si se conceden ciertos privilegios, los usuarios pueden tener la capacidad para instalar software. La organización debería identificar qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que es sólo de uso personal y software cuya procedencia se desconoce o se sospecha puede ser potencialmente maliciosa). Estos privilegios deberían asignarse en atención a las funciones de los usuarios en cuestión.

Información adicional

La instalación incontrolada de software en equipos informáticos puede llevar a introducir vulnerabilidades y, como consecuencia, a fugas de información, pérdidas de integridad y otros incidentes de seguridad de la información, o a la violación de derechos de propiedad intelectual.

12.7 Consideraciones sobre la auditoria de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

12.7.1 Controles de auditoría de sistemas de información

Control

Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberían ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.

Guía de implantación

Deberían cumplirse las siguientes directrices:

a) los requisitos de acceso de auditoría a sistemas y datos deberían acordarse con la dirección adecuada;

b) debería acordarse y controlarse el alcance de las comprobaciones técnicas de auditoría;

c) las comprobaciones deberían limitarse a accesos de sólo lectura al software y a los datos;

d) un acceso diferente al de sólo lectura debería permitirse únicamente en copias aisladas de los archivos del sistema, que deberían borrarse cuando finalice la auditoría, o a las que debería protegerse adecuadamente si es obligatorio mantener dichos archivos de acuerdo con los requisitos de documentación de la auditoría;

e) deberían identificarse y acordarse los requisitos para tratamientos especiales o adicionales;

f) las pruebas de auditoría que puedan afectar a la disponibilidad del sistema deberían ejecutarse fuera del horario laboral;

g) todos los accesos deberían ser supervisados y registrados para obtener una pista de referencia.

13 Seguridad de las comunicaciones

13.1 Gestión de la seguridad de redes

Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

13.1.1 Controles de red

Control

Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

Guía de implantación

Los controles deberían ser implementados para garantizar la seguridad de la información en las redes y la protección de servicios conectados frente a accesos no autorizados. En particular, deberían ser considerados los siguientes aspectos:

a) deberían establecerse las responsabilidades y los procedimientos para la gestión de los equipos de red;

b) la responsabilidad operacional de las redes debería estar separada de las operaciones de los sistemas informáticos donde sea apropiado (véase 6.1.2);

c) deberían establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o de redes inalámbricas y proteger los sistemas conectados y sus aplicaciones (véanse el capítulo 10 y el apartado 13.2); también podrían ser necesarios controles especiales para mantener la disponibilidad de los servicios de red y los ordenadores conectados;

d) debería realizarse un adecuado registro de eventos y monitorización para permitir el registro y detección de acciones que podrían afectar, o ser relevantes, para la seguridad de la información;

e) las actividades de gestión deberían estar estrechamente coordinadas, tanto para optimizar el servicio a la organización, como para asegurar que los controles sean aplicados consistentemente en toda la infraestructura de tratamiento de la información;

f) los sistemas de la red deberían ser autenticados;

g) la conexión de los sistemas a la red debería ser restringido.

Información adicional

Se puede encontrar información adicional sobre seguridad de la red en la Norma ISO/IEC 27033 [15][16][17][18][19].

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 y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

Guía de implantación

Se debería determinar y supervisar la capacidad del proveedor del servicio de red para gestionar los servicios acordados de una manera segura, y de igual manera, se debería acordar el derecho a ser auditado.

Se deberían identificar las disposiciones de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de gestión. La organización debería asegurar que los proveedores de servicios de red implantan estas medidas.

Información adicional

Los servicios de red incluyen la provisión de conexiones, servicios de red privada, redes de valor añadido y soluciones de seguridad de red gestionada, tales como, cortafuegos y sistemas de detección de intrusiones. Estos servicios pueden comprender desde un simple ancho de banda no gestionado hasta complejas ofertas de valor añadido.

Las características de seguridad de los servicios de red podrían ser:

a) tecnología aplicada para la seguridad de los servicios de red, tales como autenticación, cifrado y controles de conexión de red;

b) parámetros técnicos requeridos para conexiones seguras con los servicios de red de acuerdo a las reglas de seguridad y conexión a las redes;

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

13.1.3 Segregación en redes

Control

Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.

Guía de implantación

Un método para gestionar la seguridad de grandes redes es dividirlas en dominios de red separados. Los dominios pueden elegirse basándolos en niveles de confianza (por ejemplo, dominio de acceso público, dominio de puestos de usuario, dominio de servidores), junto a unidades organizativas (por ejemplo, recursos humanos, finanzas, comercial) o alguna combinación (por ejemplo, conectando un dominio de servidor a múltiples unidades organizativas). La segregación puede hacerse usando, diferentes redes físicas o diferentes redes lógicas (por ejemplo, interconexión con redes privadas virtuales).

El perímetro de cada dominio debería estar bien definido. El acceso entre dominios de red está permitido, pero debería ser controlado en el perímetro usando una pasarela (por ejemplo, cortafuegos, router de filtrado). El criterio para la segregación de redes en dominios, y el acceso permitido a través de pasarelas, debería estar basado en la evaluación de los requisitos de seguridad de cada dominio. La evaluación debería estar en conformidad con la política de control de acceso (véase 9.1.1), los requisitos de acceso, el valor y clasificación de la información procesada además de tener en cuenta el coste relativo y el impacto en el rendimiento al incorporar una pasarela con la tecnología adecuada.

Las redes inalámbricas requieren un tratamiento especial debido a la deficiente definición de su perímetro de red. Para entornos sensibles, se deberían hacer las oportunas consideraciones para tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de las redes internas hasta que el acceso haya pasado a través de la pasarela en conformidad con la política de controles de red (véase 13.1.1) antes de conceder acceso a los sistemas internos.

La autenticación, cifrado y las tecnologías de control de acceso a la red a nivel de usuario de las redes inalámbricas basadas en normas o estándares modernos podrían ser suficientes para una conexión directa a la red interna de la organización si se aplican correctamente.

Información adicional

De forma habitual, las redes se extienden más allá de los límites de la organización debido a la creación de negocios en colaboración con otras empresas que requieren la interconexión o compartición de los recursos de red para el tratamiento de información. Estas extensiones pueden aumentar el riesgo de acceso no autorizado de los sistemas de información de las organizaciones que usan la red, alguno de los cuales requerirá protección de otros usuarios de la red debido a su sensibilidad o criticidad.

13.2 Intercambio de información

Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de intercambio de información

Control

Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

Guía de implantación

Los procedimientos y controles que deberían seguirse cuando se usan recursos de comunicación para la transferencia de información deberían considerar los siguientes aspectos:

a) el diseño de procedimientos para proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción;

b) procedimientos para la detección y la protección contra el *malware* que podría ser transmitido a través del uso de comunicaciones electrónicas (véase 12.2.1);

c) procedimientos para proteger información electrónica sensible que tiene la forma de adjuntos;

d) políticas o directrices describiendo el uso aceptable de los recursos de comunicación (véase 8.1.3);

e) las responsabilidades del personal, partes externas y de cualquier otro usuario para no comprometer a la organización, por ejemplo, mediante la difamación, el acoso, la suplantación, el reenvío de mensajes en cadena, las compras no autorizadas, etc.;

f) el uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información (véase el capítulo 10);

g) directrices para la retención y eliminación de toda la correspondencia comercial, incluidos los mensajes, de acuerdo con la legislación y las reglamentaciones nacionales y locales pertinentes;

h) los controles y las restricciones asociadas con el uso de los recursos de comunicación, por ejemplo, reenvío automático del correo electrónico a las direcciones de correo externas;

i) asesorar al personal para que tome las precauciones necesarias de no revelar información confidencial;

j) no dejar mensajes que contengan información confidencial en los contestadores automáticos dado que estos podrían ser reproducidos por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como consecuencia de un error en la marcación de un teléfono;

k) asesorar al personal sobre los problemas en el uso de máquinas o servicios de fax, como:

   1) acceso no autorizado para la recuperación de mensajes almacenados,

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

   3) el envío de documentos y mensajes a un número equivocado, ya sea por error en la marcación o por el uso de un número erróneo almacenado.

Además, debería recordarse al personal que no debería tener conversaciones confidenciales en lugares públicos o usando canales de comunicación inseguros, oficinas abiertas y lugares de reunión.

Los servicios de transferencia de información deberían ajustarse a los requisitos legales pertinentes (véase 18.1).

Información adicional

La transferencia de información puede realizarse a través de un conjunto de diferentes tipos de recursos de comunicación, incluyendo correo electrónico, voz, fax y video.

La transferencia de software puede realizarse mediante un conjunto de diferentes medios, incluyendo la descarga de Internet y la adquisición de proveedores que venden productos listos para usar.

Deberían ser consideradas las implicaciones de negocio, legales y de seguridad ligadas al intercambio electrónico de datos, al comercio electrónico, las comunicaciones electrónicas y los requisitos para los controles.

13.2.2 Acuerdos de intercambio de información

Control

Deberían establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.

Guía de implantación

Los acuerdos de transferencia de información deberían incorporar lo siguiente:

a) las responsabilidades de la dirección sobre el control y la notificación de la transmisión, el envío y la recepción;

b) los procedimientos para garantizar la trazabilidad y el no repudio;

c) las normas técnicas mínimas para la compresión y el transporte;

d) los acuerdos de garantía de depósito;

e) las normas de identificación de mensajeros;

f) las responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de datos;

g) el uso de un sistema de etiquetado acordado para la información sensible o crítica, asegurando que el significado de las etiquetas se entiende de inmediato y que la información está protegida adecuadamente (véase 8.2);

h) Las normas técnicas para la grabación y la lectura de la información y el software;

i) cualquier control especial que se requiera para proteger elementos sensibles, tales como la criptografía (véase el capítulo 10);

j) el mantenimiento de una cadena de custodia de la información mientras está en tránsito;

k) los niveles aceptables de control de acceso.

Las políticas, procedimientos y normas deberían establecerse y mantenerse para proteger la información y los medios físicos en tránsito (véase 8.3.3), y debería estar referenciado en los correspondientes acuerdos de transferencia.

El contenido de la seguridad de la información de cualquier acuerdo debería reflejar la sensibilidad de la información de negocio afectada.

Información adicional

Los acuerdos pueden llevarse a cabo por vía electrónica o manual y pueden tener la forma de contratos formales. Para la información confidencial, los mecanismos específicos utilizados para la transferencia de dicha información deberían ser consistentes para todas las organizaciones y tipos de acuerdos.

13.2.3 Mensajería electrónica

Control

La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.

Guía de implantación

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

a) la protección de mensajes frente a accesos no autorizados, modificación o denegación de servicio acorde con el esquema de clasificación adoptado por la organización;

b) asegurar el correcto direccionamiento y transporte del mensaje;

c) la fiabilidad 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, tales como, mensajería instantánea, redes sociales o sistemas de compartición de ficheros;

f) mayores niveles de autenticación en el control de acceso desde redes de acceso público.

Información adicional

Existen muchos tipos de mensajería electrónica, tales como, correo electrónico, intercambio electrónico de datos y redes sociales, que desempeñan un papel importante en las comunicaciones empresariales.

13.2.4 Acuerdos de confidencialidad o no revelación

Control

Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.

Guía de implantación

Los acuerdos de confidencialidad o de no revelación deberían cubrir la necesidad de proteger la información confidencial usando términos legalmente exigibles. Los acuerdos de confidencialidad o de no revelación son aplicables, tanto a entidades externas como a empleados de la organización. Los elementos deberían seleccionarse o agregarse teniendo en cuenta el tipo de la otra parte y su acceso o el manejo permitido de la información confidencial. Para identificar los requisitos de los acuerdos de confidencialidad o de no revelación, deberían considerarse los siguientes elementos:

a) una definición de la información a proteger (por ejemplo, información confidencial);

b) la duración prevista del acuerdo, incluyendo los casos en los que la confidencialidad necesitase mantenerse indefinidamente;

c) las acciones necesarias cuando se termine un acuerdo;

d) las responsabilidades y las acciones de los firmantes para evitar la revelación no autorizada de la información;

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

f) el uso permitido de la información confidencial y los derechos del firmante para utilizar la información;

g) el derecho a auditar y supervisar las actividades que involucren información confidencial;

h) los procesos para la notificación y aviso de la revelación no autorizada o fugas de información confidencial;

i) los términos en los que la información debería ser devuelta o destruida en el cese de un acuerdo;

j) las acciones que se espera sean tomadas en caso de incumplimiento del acuerdo.

Sobre la base de los requisitos de seguridad de la información de una organización, podrían ser necesarios otros elementos en un acuerdo de confidencialidad o de no revelación.

Los acuerdos de confidencialidad y de no revelación deberían cumplir con todas las leyes y reglamentos aplicables de la jurisdicción a la que corresponda (véase 18.1).

Los requisitos para los acuerdos de confidencialidad y de no revelación deberían ser revisados periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

Información adicional

Los acuerdos de confidencialidad y no revelación protegen la información de la organización e informan a los firmantes de sus responsabilidades relativas a la protección, utilización y revelación de información de una manera responsable y autorizada.

Una organización podría necesitar utilizar tipos de acuerdos de confidencialidad o de no revelación distintos para diferentes circunstancias.

14 Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1 Requisitos de seguridad en los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información

Control

Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Guía de implantación

Se deberían identificar requisitos de seguridad de la información mediante diversos métodos, tales como los derivados del cumplimiento de políticas y normativas, del modelado de amenazas, de la evaluación de incidentes o del uso de umbrales de vulnerabilidad. Los resultados de la identificación de requisitos deberían ser documentados y revisados por todas las partes interesadas.

Los requisitos y controles de seguridad de la información deberían reflejar el valor empresarial de la información involucrada (véase 8.2) y el potencial impacto negativo en el negocio que pudiera derivarse de la falta de una seguridad adecuada.

La identificación y gestión de los requisitos de seguridad de la información y de los procesos asociados deberían integrarse 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 dar lugar a soluciones más eficaces y eficientes en costes.

Los requisitos de seguridad de la información también deberían considerar:

a) el nivel de confianza necesario en la identidad declarada de los usuarios, a fin de obtener los requisitos de autenticación de usuario;

b) los procesos de aprobación y autorización de acceso, tanto para los usuarios del negocio como para los usuarios con privilegios o usuarios técnicos;

c) la información a los usuarios y operadores de sus deberes y responsabilidades;

d) las necesidades de protección requeridas para los activos involucrados, en particular respecto a la disponibilidad, la confidencialidad y la integridad;

e) los requisitos derivados de los procesos de negocio, tales como el registro y monitorización de transacciones y requisitos de no repudio;

f) los requisitos impuestos por otros controles de seguridad, por ejemplo, interfaces para el registro y la monitorización o sistemas de detección de fugas de datos.

Para las aplicaciones que ofrecen servicios a través de redes públicas o que realizan transacciones, se deberían considerar los controles dedicados 14.1.2 y 14.1.3.

Si los productos son adquiridos, se debería seguir un proceso de pruebas y adquisición formal. Los contratos con el proveedor deberían cubrir los requisitos de seguridad identificados. Cuando las funciones de seguridad propuestas en un producto no satisfacen los requisitos especificados, se debería reconsiderar el riesgo que introduce y los controles asociados antes de comprar el producto.

Se deberían evaluar e implantar las guías disponibles para la configuración de la seguridad del producto, alineada con el software y los servicios finales.

Se deberían definir criterios para la aceptación de los productos, por ejemplo, en cuanto a su funcionalidad, que asegurarán el cumplimiento de los requisitos de seguridad identificados. Los productos deberían ser evaluados en relación con estos criterios antes de la adquisición. Las funcionalidades adicionales deberían ser revisadas para asegurarse de que no presentan nuevos riesgos inaceptables.

Información adicional

Las Normas ISO/IEC 27005[11] e ISO 31000[27] proporcionan orientación sobre el uso de los procesos de gestión de riesgos para identificar controles para cumplir con los requisitos de seguridad de la información.

14.1.2 Asegurar los servicios de aplicaciones en redes públicas

Control

La información involucrada en aplicaciones que pasan a través de redes públicas debería ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.

Guía de implantación

Las consideraciones sobre la seguridad de la información para los servicios de aplicaciones que se transmiten a través de redes públicas deberían incluir lo siguiente:

a) el nivel de confianza que cada parte requiere de la identidad declarada del otro, por ejemplo, a través de la autenticación;

b) los procesos de autorización asociados con quién puede aprobar, emitir o firmar documentos transaccionales clave;

c) la garantía de que las partes en comunicación están plenamente informadas de sus autorizaciones para la prestación o uso del servicio;

d) el establecimiento y acuerdo sobre los requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio de los contratos, por ejemplo, asociado a los procesos de licitación y contratación;

e) el nivel de confianza requerido para la integridad de los documentos clave;

f) los requisitos de protección de la información confidencial;

g) la confidencialidad y la integridad de las transacciones de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de los recibos de entrega;

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

i) la selección de la forma de pago más adecuada para evitar el fraude;

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

k) evitar la pérdida o duplicación de información de la transacción;

l) la responsabilidad asociada con cualquier transacción fraudulenta;

m) los requisitos de los seguros.

Muchas de las consideraciones anteriores se pueden resolver mediante la aplicación de controles criptográficos (véase el capítulo 10), teniendo en cuenta el cumplimiento de los requisitos legales (véase el capítulo 18, especialmente 18.1.5 acerca de la legislación sobre criptografía).

Los acuerdos de servicios de aplicaciones entre socios deberían estar respaldadas por un acuerdo documentado que comprometa a ambas partes en los términos acordados para los servicios, incluidos los detalles de la autorización (véase punto b) anterior).

Se deberían considerar requisitos de resiliencia frente a los ataques, lo que puede incluir requisitos para la protección de los servidores de aplicaciones involucrados o asegurar la disponibilidad de las interconexiones de red necesarias para prestar el servicio.

Información adicional

Las aplicaciones accesibles a través de redes públicas están sujetas a una serie de amenazas relacionadas con la red, tales como actividades fraudulentas, disputas de contratos o la divulgación de información al público. Por lo tanto, son indispensables las evaluaciones detalladas del riesgo y la selección adecuada de controles. Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y el aseguramiento de la transferencia de datos.

Los servicios de aplicaciones pueden hacer uso de métodos de autenticación seguros, por ejemplo, utilizando criptografía de clave pública y firmas digitales (véase el capítulo 10) para reducir los riesgos. Además, se pueden utilizar terceros de confianza donde sean necesarios tales servicios.

14.1.3 Protección de las transacciones de servicios de aplicaciones

Control

La información involucrada en las transacciones de servicios de aplicaciones debería ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.

Guía de implantación

Las consideraciones sobre la seguridad de la información en las transacciones de servicios de aplicaciones deberían incluir lo siguiente:

a) la utilización de firmas electrónicas para cada una de las partes involucradas en la transacción;

b) considerar todos los aspectos de la transacción, es decir, garantizar que:

   1) la información secreta de autenticación de los usuarios de todas las partes es válida y verificada,

   2) la transacción permanezca confidencial,

   3) la privacidad asociada con todas las partes involucradas se mantiene;

c) rutas de comunicación cifradas entre todas las partes involucradas;

d) protocolos seguros utilizados para la comunicación entre todas las partes involucradas;

e) garantizar que el almacenamiento de los detalles de la transacción se encuentra fuera de cualquier entorno de acceso público, por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no se mantiene y está expuesta en un medio de almacenamiento accesible directamente desde Internet;

f) cuando se utiliza una autoridad de confianza (por ejemplo, para la expedición y el mantenimiento de las firmas digitales o certificados digitales), la seguridad está integrada y embebida en todo el proceso de gestión, extremo a extremo, de certificados/firmas.

Información adicional

La extensión de los controles previstos debería ser proporcional al nivel de riesgo asociado a cada tipo de transacción de los servicios de las aplicaciones.

Las transacciones pueden tener que cumplir con requisitos legales y reglamentarios de la jurisdicción dónde se genera la transacción, se procesa, se completa o se almacena.

14.2 Seguridad en el desarrollo y en los procesos de soporte

Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.

14.2.1 Política de desarrollo seguro

Control

Se deberían establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.

Guía de implantación

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguros. Dentro de una política de desarrollo seguro, se deberían someter a consideración los siguientes aspectos:

a) la seguridad del entorno de desarrollo;

b) directrices sobre la seguridad en el ciclo de vida de desarrollo de software:

   1) seguridad en la metodología de desarrollo de software,

   2) guías de desarrollo seguro para cada lenguaje de programación utilizado,

c) requisitos de seguridad en la fase de diseño;

d) puntos de verificación de seguridad incorporados a los hitos del proyecto;

e) repositorios seguros;

f) seguridad en el control de versiones;

g) conocimiento necesario sobre seguridad de aplicaciones;

h) capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades.

Se deberían utilizar técnicas de programación segura tanto para los nuevos desarrollos, como en las situaciones de reutilización de código, donde las normas aplicadas al desarrollo pudieron no ser conocidas o no estaban en consonancia con las mejores prácticas actuales. Se deberían considerar normas de programación segura y las indicaciones correspondientes para su uso. Los desarrolladores deberían ser formados en su uso y las pruebas y la revisión de código deberían verificar que han sido aplicadas.

Si el desarrollo se subcontrata, la organización debería asegurarse de que la parte externa cumple con estas normas para el desarrollo seguro (véase 14.2.7).

Información adicional

El desarrollo también puede tener lugar dentro de las aplicaciones, como las aplicaciones de ofimática, de generación de sentencias, navegadores y bases de datos.

14.2.2 Procedimiento de control de cambios en sistemas

Control

La implantación de cambios a lo largo del ciclo de vida del desarrollo debería controlarse mediante el uso de procedimientos formales de control de cambios.

Guía de implantación

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir, tanto en las primeras etapas del diseño como en los mantenimientos posteriores, para asegurar la integridad del sistema, de las aplicaciones y de los productos. La incorporación de nuevos sistemas y cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificaciones, pruebas, control de calidad y gestión de la implantación.

Este proceso debería incluir una evaluación del riesgo, el análisis de los impactos de los cambios y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurarse de que los procedimientos de seguridad y de control existentes no se vean comprometidos, que a los programadores de apoyo se les da acceso sólo a aquellas partes del sistema necesarias para su trabajo y que se obtiene el acuerdo formal y la aprobación de cualquier cambio.

Siempre que sea posible, los procedimientos de control de cambios operacionales y de cambios de aplicación deberían integrarse (véase 12.1.2). Los procedimientos de control de cambios deberían incluir, pero no limitarse a:

a) el mantenimiento de un registro de los niveles de autorización aprobados;

b) asegurar que los cambios son enviados a los usuarios autorizados;

c) la revisión de los controles y procedimientos de integridad para asegurar que no se verán comprometidos por los cambios;

d) la identificación de todo el software, la información, las entidades de base de datos y el hardware que requieren cambios;

e) la identificación y comprobación de la seguridad del código crítico para minimizar la probabilidad de fallos de seguridad conocidos;

f) la aprobación formal de propuestas detalladas antes de que comience el trabajo;

g) la aceptación de los cambios por los usuarios autorizados antes de la implantación;

h) la actualización del conjunto de la documentación del sistema a la finalización de cada cambio y el archivo o eliminación de la documentación obsoleta;

i) el mantenimiento de un control de versiones para todas las actualizaciones de software;

j) el mantenimiento de registros de auditoría de todas las solicitudes de cambio;

k) la adaptación de la documentación operativa (véase 12.1.1) y de los procedimientos de usuario, según sea necesario, para que sigan siendo apropiadas;

l) la implantación de los cambios en el momento adecuado de forma que no perturbe los procesos de negocio involucrados.

Información adicional

El cambio de software puede afectar el entorno de operación y viceversa.

Las buenas prácticas incluyen las pruebas del nuevo software en un entorno segregado de los entornos de explotación y desarrollo (véase 12.1.4). Esto proporciona control sobre el nuevo software y permite una protección adicional de la información operacional que se utiliza para las pruebas. Esto debería aplicarse incluso a parches, service packs y otras actualizaciones.

Cuando se consideren actualizaciones automáticas, debería ser sopesado el riesgo para la integridad y la disponibilidad del sistema frente al beneficio de la rápida implantación de las actualizaciones. Los cambios automáticos no deberían utilizarse en sistemas críticos, ya que algunos cambios pueden hacer que las aplicaciones críticas fallen.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Control

Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deberían ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.

Guía de implantación

Este proceso debería incluir:

a) la revisión de los procedimientos de control y de integridad de las aplicaciones para asegurarse de que no han sido comprometidos por los cambios en los sistemas operativos;

b) la garantía de que los cambios en los sistemas operativos están previstos en un plazo que permita realizar pruebas y revisiones antes de la implantación;

c) la realización los cambios necesarios en los planes de continuidad del negocio (véase el capítulo 17).

Información adicional

Las plataformas de operación incluyen sistemas operativos, bases de datos y sistemas *middleware*. El control también se debería aplicar a los cambios de las aplicaciones.

14.2.4 Restricciones a los cambios en los paquetes de software

Control

Se deberían desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deberían ser objeto de un control riguroso.

Guía de implantación

En la medida de lo posible, los paquetes de software suministrados por el proveedor deberían usarse sin modificaciones. Cuando un paquete de software se necesite modificar, se deberían considerar los siguientes puntos:

a) el riesgo de que los controles y los procesos de integridad incorporados se vean comprometidos;

b) la necesidad de obtener el consentimiento del proveedor;

c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones del programa estándar;

d) el impacto producido si la organización se convierte en responsable del mantenimiento futuro del software como resultado de los cambios;

e) la compatibilidad con otro software en uso.

Si los cambios son necesarios, se debería conservar el software original y los cambios se aplicarán a una copia identificada. Se debería implementar un proceso de gestión de actualizaciones de software para asegurar que se instalan las actualizaciones de los parches aprobados y de todo el software autorizado (véase 12.6.1). Todas las modificaciones deberían ser completamente probadas y documentadas, para el caso de que tengan que volver a aplicarse, si fuera necesario, a actualizaciones futuras del software. Si se considera necesario, las modificaciones deberían ser probadas y validadas por un organismo de evaluación independiente.

14.2.5 Principios de ingeniería de sistemas seguros

Control

Principios de ingeniería de sistemas seguros se deberían establecer, documentar, mantener y aplicarse a todos los esfuerzos de implantación de sistemas de información.

Guía de implantación

Se deberían establecer y documentar procedimientos de ingeniería de sistemas de información seguros basándose en los principios de ingeniería de seguridad y aplicarse a las actividades de ingeniería de sistemas de información internos. La seguridad se debería diseñar en todas las capas de la arquitectura (de negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de la información con la necesidad de accesibilidad. Se deberían analizar los riesgos de seguridad de las nuevas tecnologías y se debería revisar el diseño contra los patrones de ataque conocidos.

Estos principios y los procedimientos de ingeniería establecidos deberían revisarse periódicamente para asegurarse de que están contribuyendo de manera efectiva a la mejora de las normas de seguridad en los procesos de ingeniería. Se deberían revisar periódicamente para asegurarse de que permanecen actualizados en cuanto a la lucha contra las nuevas amenazas potenciales y que siguen siendo aplicables a los avances en las tecnologías y soluciones a las que se aplica.

Los principios de ingeniería de seguridad establecidos deberían aplicarse, en su caso, a los sistemas de información externos a través de los contratos y otros acuerdos vinculantes entre la organización y el proveedor al que la organización subcontrata. La organización debería confirmar que el rigor de los principios de ingeniería de seguridad de los proveedores es comparable con el suyo.

Información adicional

Los procedimientos de desarrollo de aplicaciones deberían aplicar técnicas de ingeniería de seguridad en el desarrollo de aplicaciones que tienen interfaces de entrada y salida. Las técnicas de ingeniería de seguridad ofrecen orientación sobre las técnicas de autenticación de usuario, control de sesión segura, validación y depuración de datos, y eliminación de códigos de depuración.

14.2.6 Entorno de desarrollo seguro

Control

Las organizaciones deberían establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

Guía de implantación

Un entorno de desarrollo seguro incluye las personas, los procesos y la tecnología relacionados con el desarrollo e integración de sistemas.

Las organizaciones deberían evaluar los riesgos asociados con los proyectos de desarrollo de sistemas individuales y establecer entornos de desarrollo seguros para los proyectos específicos de desarrollo del sistema, teniendo en cuenta:

a) la sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema;

b) los requisitos externos e internos aplicables, por ejemplo, de reglamentos o políticas;

c) los controles de seguridad ya implementados por la organización que apoyen el desarrollo del sistema;

d) la honradez del personal que trabaja en el entorno (véase 7.1.1);

e) el grado de contratación externa asociada con el desarrollo del sistema;

f) la necesidad de la segregación entre los diferentes entornos de desarrollo;

g) el control de accesos al entorno de desarrollo;

h) la monitorización de los cambios en el entorno y el código almacenado en el mismo;

i) el almacenamiento seguro de las copias de respaldo fuera de las instalaciones;

j) el control del movimiento de datos desde y hacia el entorno.

Una vez que el nivel de protección se determina para un entorno de desarrollo específico, las organizaciones deberían documentar los procesos correspondientes en los procedimientos de desarrollo seguro y proporcionarlos a todos los individuos que los necesiten.

14.2.7 Externalización del desarrollo de software

Control

El desarrollo de software externalizado debería ser supervisado y controlado por la organización.

Guía de implantación

Cuando se subcontrata el desarrollo del sistema, se deberían considerar los siguientes puntos a través de toda la cadena de suministro externo a la organización:

a) los acuerdos de licencias, la propiedad del código y los derechos de propiedad intelectual relacionados con los contenidos subcontratados (véase 18.1.2);

b) los requisitos contractuales para las prácticas de diseño seguro, codificación y pruebas (véase 14.2.1);

c) la entrega del modelo de amenazas aprobado al desarrollador externo;

d) las pruebas de aceptación de calidad y la adecuación de las entregas;

e) la presentación de pruebas de que los umbrales de seguridad se utilizan para establecer los niveles mínimos aceptables de seguridad y calidad de la privacidad;

f) la presentación de pruebas de que se han realizado suficientes pruebas para proteger contra la presencia en los entregables de contenido malicioso, tanto intencionado como no intencionado;

g) la presentación de pruebas de que se han realizado suficientes pruebas para proteger contra la presencia de vulnerabilidades conocidas;

h) los acuerdos de depósito en garantía, por ejemplo, si el código fuente no está disponible;

i) el derecho contractual para auditar procesos y controles de desarrollo;

j) la documentación real del entorno de compilación utilizado para crear los entregables;

k) la organización sigue siendo responsable de cumplir con las leyes aplicables y la verificación de la eficacia del control.

Información adicional

Se puede encontrar más información sobre relaciones con los proveedores en la Norma ISO/IEC 27036 [21] [22] [23].

14.2.8 Pruebas funcionales de seguridad de sistemas

Control

Se deberían llevar a cabo pruebas de la seguridad funcional durante el desarrollo.

Guía de implantación

Los sistemas nuevos y los actualizados requieren pruebas y verificación exhaustivas en los procesos de desarrollo, incluyendo la preparación de un programa detallado de actividades y datos de prueba junto a los resultados esperados bajo las condiciones establecidas. Para desarrollos propios, dichas pruebas inicialmente deberían ser realizadas por el equipo de desarrollo. Se deberían realizar pruebas de aceptación independientes (tanto en los desarrollos internos como para los desarrollos externalizados) para asegurar que el sistema funciona como se esperaba y sólo como se esperaba (véase 14.1.1 y 14.2.9). La extensión de las pruebas debería ser proporcional a la importancia y la naturaleza del sistema.

14.2.9 Pruebas de aceptación de sistemas

Control

Se deberían establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

Guía de implantación

Las pruebas de aceptación del sistema deberían incluir las pruebas de los requisitos de seguridad de la información (véase 14.1.1 y 14.1.2) y de que se han aplicado las prácticas de desarrollo seguro del sistema (véase 14.2.1). Las pruebas también deberían llevarse a cabo sobre los componentes recibidos y los sistemas integrados. Las organizaciones pueden utilizar herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidad, y verificar la solución de los defectos relacionados con la seguridad.

Las pruebas deberían realizarse en un entorno de prueba realista para asegurar que el sistema no va a introducir vulnerabilidades al entorno de la organización y que las pruebas son fiables.

14.3 Datos de prueba

Objetivo: Asegurar la protección de los datos de prueba.

14.3.1 Protección de los datos de prueba

Control

Los datos de prueba se deberían seleccionar con cuidado y deberían ser protegidos y controlados.

Guía de implantación

Se debería evitar el uso de datos reales de operación que contengan datos personales o cualquier otra información confidencial para las pruebas. Si se utiliza la información de datos personales o información confidencial para las pruebas, todos los detalles y contenidos sensibles deberían protegerse mediante su retirada o su modificación (véase la Norma ISO/IEC 29101[26]).

Se deberían aplicar las siguientes directrices para proteger los datos de operación cuando se usan para las pruebas:

a) los procedimientos de control de acceso que se aplican a los sistemas de aplicaciones operacionales, deberían aplicarse también en los sistemas de pruebas;

b) debería haber una autorización independiente cada vez que la información de operación se copia en un entorno de prueba;

c) la información operacional se debería borrar del entorno de prueba inmediatamente después que la prueba se haya completado;

d) la copia y utilización de información operacional deberían ser registrada para proporcionar evidencias de auditoría.

Información adicional

Los sistemas y pruebas de aceptación normalmente requieren importantes volúmenes de datos de prueba que sean tan reales como sea posible.

15 Relación con proveedores

15.1 Seguridad en las relaciones con 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 en las relaciones con los proveedores

Control

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deberían acordarse con el proveedor y quedar documentados.

Guía de implantación

La organización debería identificar y encargar los controles de seguridad de información para abordar específicamente el acceso de los proveedores a la información de la organización en una política. Estos controles deberían cubrir los procesos y procedimientos a ser implantados por la organización, así como aquellos procesos y procedimientos que la organización debería requerir implantar al proveedor, incluyendo:

a) la identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, servicios de logística, servicios financieros, componentes de la infraestructura de TI, a los cuales la organización permitirá acceder a su información;

b) un proceso y un ciclo de vida normalizados para la gestión de las relaciones con los proveedores;

c) definir los tipos de acceso a la información que se permitirá a los diferentes tipos de proveedores, con su supervisión y su control del acceso;

d) los requisitos mínimos de seguridad de la información por cada tipo de información y tipo de acceso para servir de base para cada uno de los acuerdos con los proveedores en consonancia con las necesidades y requisitos de negocio de la organización y su perfil de riesgo;

e) los procesos y procedimientos para supervisar el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y cada tipo de acceso, incluyendo la revisión por terceros y la validación de los productos;

f) los controles de exactitud y completitud, para garantizar la integridad de la información o del tratamiento de la información proporcionados por cualquiera de las partes;

g) los diferentes tipos de obligaciones que sean aplicables a los proveedores para proteger la información de la organización;

h) la gestión de incidencias y contingencias asociadas al acceso de los proveedores, incluyendo responsabilidades, tanto de la organización, como de los proveedores;

i) los acuerdos de resiliencia y, si fuesen necesarios, acuerdos de recuperación y de contingencia para asegurar la disponibilidad de la información o el tratamiento de la información proporcionada por cualquiera de las partes;

j) las sesiones de concienciación para el personal de la organización que participa en compras con respecto a las políticas, procesos y procedimientos aplicables;

k) las sesiones de concienciación para el personal de la organización que interactúa con el personal de los proveedores con respecto a las reglas apropiadas referentes al acuerdo y a las actuaciones según el tipo de proveedor y el nivel de acceso de proveedores a los sistemas y la información de la organización;

l) las condiciones bajo las que los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;

m) la gestión de las migraciones necesarias de información, instalaciones de tratamiento de la información y cualquier otra cosa que necesite ser migrada, y garantizar que la seguridad de información se mantenga durante todo el período de transición.

Información adicional

Los proveedores pueden poner en riesgo la información con una gestión inadecuada de la seguridad de la información. Deberían identificarse y aplicarse controles para administrar el acceso de proveedores a las instalaciones de tratamiento de la información. Por ejemplo, si hay una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no revelación. Otro ejemplo es el riesgo sobre protección de los datos cuando el acuerdo con el proveedor implica la transferencia o el acceso a la información a nivel internacional. La organización tiene que ser consciente de que la responsabilidad, legal o contractual, para proteger la información permanece en la organización.

15.1.2 Requisitos de seguridad en contratos con terceros

Control

Todos los requisitos relacionados con la seguridad de la información deberían establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura "Tecnología de la Información".

Guía de implantación

Se deberían establecer y documentar los acuerdos con los proveedores para asegurar que no haya malentendidos entre la organización y el proveedor respecto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

Se deberían considerar las siguientes cuestiones para su inclusión en los acuerdos con el fin de satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información facilitada o accedida, y los métodos para facilitar o acceder a la información;

b) la clasificación de la información de acuerdo con el esquema de clasificación de la organización (véase 8.2); si es necesario también, relacionar el propio esquema de clasificación de la organización con el sistema de clasificación del proveedor;

c) los requisitos legales y regulatorios, incluyendo la protección de datos personales, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se garantizará que se cumplen;

d) la obligación contractual de cada parte para implementar un conjunto acordado de controles incluyendo el control de acceso, la evaluación del desempeño, la supervisión, los informes y la auditoría;

e) normas sobre el uso aceptable de la información, incluyendo el uso inaceptable, si fuese necesario;

f) cualquier lista explícita de personal del proveedor autorizado para acceder o recibir información de la organización, los procedimientos y las condiciones de la autorización, y la baja de la autorización para el acceso o recepción de información de la organización por parte del personal del proveedor;

g) políticas de seguridad de la información relevantes para el contrato específico;

h) requisitos y procedimientos de gestión de incidentes (en especial de notificación y colaboración durante la corrección de los incidentes);

i) la formación y concienciación sobre los requisitos de procedimientos específicos y requisitos de seguridad de la información, por ejemplo para la respuesta a incidentes, o para los procedimientos de autorización;

j) los reglamentos pertinentes para la subcontratación, incluidos los controles que necesiten ser implantados;

k) acuerdos pertinentes de colaboración, incluyendo una persona de contacto para los asuntos de seguridad de la información;

l) requisitos de investigación del personal, si los hubiere, para el personal del proveedor, incluyendo responsabilidades para llevar a cabo la investigación, con procedimientos de notificación si la investigación no se ha completado o si los resultados son motivo de duda o preocupación;

m) derecho de auditar los procesos de los proveedores y los controles relacionados con el acuerdo;

n) procesos de resolución de contrato por defecto y por conflictos;

o) la obligación del proveedor de entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de las cuestiones relevantes indicadas en el informe;

p) las obligaciones de los proveedores para cumplir con los requisitos de seguridad de la organización.

Información adicional

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de proveedores. Por lo tanto, se debería tener cuidado en incluir todos los riesgos y requisitos de seguridad de la información pertinentes. Los acuerdos con proveedores también pueden involucrar a otras partes (por ejemplo, sub-contratistas).

Se deberían considerar en el acuerdo los procedimientos para la continuidad de servicios, en el caso de que el proveedor sea incapaz de suministrar sus productos o servicios, para evitar cualquier retraso en organizar la sustitución prevista de los productos o servicios.

15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

Control

Los acuerdos con proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

Guía de implantación

Las siguientes cuestiones deberían considerarse para su inclusión en los acuerdos con los proveedores en relación a la seguridad de la cadena de suministro:

a) la definición de requisitos de seguridad de la información para aplicar a la compra de productos o servicios de Tecnología de la Información y de las Comunicaciones (en adelante TIC), además de los requisitos de seguridad de la información generales de relaciones con los proveedores;

b) para los servicios TIC, se requiere que los proveedores reproduzcan los requisitos de seguridad de la organización a lo largo de su cadena de suministro si los proveedores subcontratan partes de los servicios TIC proporcionados a la organización;

c) para productos TIC, se requiere que los proveedores reproduzcan las apropiadas prácticas de seguridad en toda la cadena de suministro, si dichos productos incluyen componentes comprados a otros proveedores;

d) la implantación de un proceso de supervisión y métodos aceptables para validar que los productos y servicios TIC entregados cumplan con los requisitos de seguridad establecidos;

e) la implantación de un proceso de identificación de componentes críticos de productos o servicios para el mantenimiento de la funcionalidad y que, por tanto, requieren una mayor atención y control cuando se construyen fuera de la organización, especialmente si el proveedor principal subcontrata partes del producto o componentes del servicio a otros proveedores;

f) obtener garantías de que los componentes críticos y su origen se pueden trazar a lo largo de la cadena de suministro;

g) obtener garantías de que los productos TIC suministrados funcionan como se espera sin ningún tipo de características inesperadas o no deseadas;

h) la definición de reglas para el intercambio de información con respecto a la cadena de suministro y la gestión de posibles problemas y compromisos entre la organización y los proveedores;

i) la implantación de procesos específicos para la gestión de la información y el ciclo de vida, la disponibilidad y los riesgos de seguridad asociados a los componentes TIC. Esto incluye la gestión de los riesgos del fin de la disponibilidad de los componentes, debido al cese de negocio de los proveedores, o a que los proveedores no entreguen ya estos componentes por obsolescencia tecnológica.

Información adicional

Las prácticas específicas de gestión de riesgos de la cadena de suministro TIC se construyen sobre las prácticas de seguridad de la información en general, de calidad, gestión de proyectos e ingeniería del sistema, pero no las reemplazan.

Se recomienda a las organizaciones trabajar con los proveedores para entender la cadena de suministro TIC y todas las cuestiones que tienen un impacto importante sobre los productos y servicios que se proporcionen. Las organizaciones pueden influir en las prácticas de seguridad de la información de la cadena de suministro TIC, dejando claro en los acuerdos con sus proveedores, los asuntos que deberían ser abordados por otros proveedores en la cadena de suministro TIC.

Esta cadena de suministro TIC incluye los servicios informáticos en la "nube" (*cloud computing*).

15.2 Gestión de la provisión de servicios del proveedor

Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

15.2.1 Control y revisión de la provisión de servicios del proveedor

Control

Las organizaciones deberían controlar, revisar y auditar regularmente la provisión de servicios del proveedor.

Guía de implantación

La supervisión y la revisión de los servicios de proveedores deberían asegurar que los términos y las condiciones de seguridad de la información de los acuerdos se están cumpliendo y que los incidentes y problemas de seguridad de la información se gestionan adecuadamente.

Esto debería incluir un proceso de gestión del servicio entre la organización y el proveedor para:

a) supervisar los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos;

b) revisar los informes del servicio producidos por el proveedor y organizar reuniones periódicas de progreso según sea requerido en los acuerdos;

c) llevar a cabo auditorías de los proveedores, junto con la revisión de los informes de auditoría independiente, si están disponibles, y el seguimiento de las cuestiones identificadas;

d) proporcionar información sobre los incidentes de seguridad de la información y revisar esta información según sea requerido en los acuerdos y las directrices y procedimientos de soporte;

e) revisar las pistas de auditoría de los proveedores y los registros de eventos de seguridad de la información, problemas operativos, fallos, registro de los errores e interrupciones relacionados con el servicio prestado;

f) resolver y gestionar cualquier problema detectado;

g) revisar los aspectos de seguridad de la información en las relaciones del proveedor con sus propios proveedores;

h) asegurar que el proveedor mantenga la capacidad de servicio suficiente, junto con planes viables destinados a garantizar que los niveles de continuidad de servicio acordados se mantengan después de fallos mayores de los servicios o de desastre (véase el capítulo 17).

La responsabilidad de la gestión de las relaciones con los proveedores se debería asignar a una persona individual o al equipo de gestión del servicio. Además, la organización debería asegurarse de que los proveedores asignen responsabilidades internas para revisar el cumplimiento y la aplicación de los requisitos de los acuerdos. Deberían estar disponibles los suficientes recursos técnicos para supervisar, en particular, que se están cumpliendo los requisitos de seguridad de la información del acuerdo. Se deberían tomar las medidas apropiadas cuando se observan deficiencias en la prestación de servicios.

La organización debería mantener suficiente control y visibilidad general sobre todos los aspectos de seguridad de la información o de las instalaciones de tratamiento de la información, sensibles o críticas, que se acceden, procesan o gestionan por un proveedor. La organización debería mantener la visibilidad de las actividades de seguridad, tales como la gestión del cambio, la identificación de las vulnerabilidades y la notificación de incidentes de seguridad de información y la respuesta a través de un proceso definido de reporte.

15.2.2 Gestión de cambios en la provisión del servicio del proveedor

Control

Se deberían gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.

Guía de implantación

Los siguientes aspectos se deberían tener en consideración:

a) cambios en los acuerdos con los proveedores;

b) cambios realizados por la organización para implementar:

   1) mejoras en los servicios actuales ofrecidos,

   2) desarrollo de nuevas aplicaciones y nuevos sistemas,

   3) modificaciones o actualizaciones de las políticas y procedimientos de la organización,

   4) controles nuevos o modificados para resolver los incidentes de seguridad de la información y para mejorar la seguridad;

c) cambios en los servicios de los proveedores para implementar:

   1) cambios y mejora de las redes,

   2) el uso de nuevas tecnologías,

   3) la adopción de nuevos productos o nuevas versiones,

   4) nuevas herramientas y entornos de desarrollo,

   5) cambios en la ubicación física de las instalaciones de servicios,

   6) el cambio de proveedores,

   7) subcontratación a otro proveedor.

16 Gestión de incidentes de seguridad de la información

16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

Guía de implantación

Deberían tenerse en cuenta las siguientes directrices en los procedimientos de gestión de los incidentes de seguridad de la información:

a) deberían establecerse responsabilidades a nivel de gestión para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:

   1) procedimientos para la planificación y preparación de la respuesta a incidentes,

   2) procedimientos para monitorizar, detectar, analizar y comunicar eventos e incidentes de seguridad de la información,

   3) procedimientos para registrar las actividades de gestión de incidentes,

   4) procedimientos para el manejo de pruebas forenses,

   5) procedimientos para evaluar y tomar decisiones sobre eventos de seguridad y evaluar puntos débiles de la seguridad de la información,

   6) procedimientos de respuesta incluyendo aquellos relativos al escalado, recuperación controlada a partir de un incidente, y comunicación a personas internas y externas o a terceras organizaciones;

b) se deberían establecer procedimientos que aseguren que:

   1) personal competente maneja los asuntos relacionados con los incidentes de seguridad de la información dentro de la organización,

   2) se implante un punto de contacto para la detección y comunicación de incidentes de seguridad,

   3) se mantienen contactos apropiados con las autoridades, grupos de interés externos o foros que tratan asuntos relacionados con los incidentes de seguridad de la información;

c) los procedimientos de comunicación deberían incluir:

   1) la preparación de formularios de comunicación de eventos de seguridad de la información para apoyar la acción de comunicación y para ayudar a la persona que los comunique a recordar todas las acciones necesarias en caso de un evento de seguridad de la información,

   2) el comportamiento adecuado que debería tomarse en caso de un evento de seguridad de la información; por ejemplo, anotar inmediatamente todos los detalles importantes (como el tipo de incumplimiento, fallo de funcionamiento, mensajes en la pantalla...), informar inmediatamente al punto de contacto, y adoptar sólo acciones coordinadas,

3) la referencia a un proceso disciplinario formal establecido para tratar a los trabajadores, contratistas o terceros que hayan cometido el quebrantamiento de la seguridad,

4) procesos de retroalimentación adecuados para garantizar que aquellas personas que comuniquen eventos de seguridad de la información son informadas de los resultados después de que se haya tratado y cerrado el problema.

Los objetivos de la gestión de incidentes de seguridad de la información deberían ser acordados con la dirección, y debería garantizarse que los responsables de la gestión de incidentes de seguridad de la información comprenden las prioridades de la organización en cuanto al tratamiento de los incidentes de seguridad de la información.

Información adicional

Los incidentes de seguridad de la información pueden trascender los límites de la organización o del país. Para reaccionar ante dichos incidentes, resulta cada vez más necesario coordinar la respuesta y compartir la información acerca de estos incidentes con organizaciones externas, cuando esto sea apropiado.

Una guía detallada sobre la gestión de incidentes de seguridad de la información está disponible en la Norma ISO/IEC 27035[20].

16.1.2 Notificación de los eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.

Guía de implantación

Todos los trabajadores, contratistas y terceros deberían conocer su responsabilidad de comunicar cualquier evento de seguridad de la información lo antes posible. También deberían conocer el procedimiento de comunicación de eventos de seguridad de la información y el punto de contacto.

Se considerarán como situaciones para comunicar eventos de seguridad de la información las siguientes:

a) control ineficaz de la seguridad;

b) quebrantamiento de las expectativas de integridad, confidencialidad y disponibilidad de la información;

c) errores humanos;

d) incumplimientos de políticas o directrices;

e) quebrantamientos de las directrices de seguridad física;

f) cambios incontrolados del sistema;

g) disfunciones del software o hardware;

h) violaciones de acceso.

Información adicional

Disfunciones u otros comportamientos anómalos del sistema pueden ser un indicador de un ataque de seguridad o una brecha de seguridad y deberían ser comunicados siempre como un evento de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad

Control

Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

Guía de implantación

Todos los trabajadores y contratistas deberían comunicar estos incidentes a su punto de contacto lo antes posible para evitar incidentes de seguridad de la información. El mecanismo de comunicación debería ser todo lo fácil, accesible y disponible que sea posible.

Información adicional

Todos los empleados y contratistas deberían estar informados de que en ningún caso deberían intentar comprobar un punto débil que sospechen que exista. Si lo hacen, esto podría interpretarse como un posible uso indebido del sistema y podría asimismo provocar daños en el sistema o servicio de información, lo que podría derivar en responsabilidades legales para la persona que haya realizado la comprobación.

16.1.4 Evaluación y decisión sobre los eventos de seguridad de información

Control

Los eventos de seguridad de la información deberían ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la información.

Guía de implantación

El punto de contacto debería evaluar cada evento de seguridad de la información recurriendo a la escala de clasificación de eventos e incidentes de seguridad establecida y decidir si el evento debería clasificarse como incidente de seguridad de la información. La clasificación y priorización de incidentes puede ayudar a identificar el impacto y extensión de un incidente.

En casos donde la organización tiene un equipo de respuesta a incidentes de seguridad de la información (*Information Security Incident Response Team*, ISIRT), la evaluación y decisión puede redirigirse al equipo para su confirmación o reevaluación.

Los resultados de la evaluación y decisión deberían registrarse con todo detalle a efectos de futuras referencias y verificación.

16.1.5 Respuesta a incidentes de seguridad de la información

Control

Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.

Guía de implantación

Los incidentes de seguridad de la información deberían ser comunicados para su respuesta a un punto de contacto preestablecido así como a otras personas relevantes de la organización o terceras partes (véase 16.1.1).

La respuesta debería incluir los siguientes procedimientos:

a) recogida de evidencias tan pronto como sea posible tras la ocurrencia del incidente;

b) realización de un análisis forense de la seguridad de la información según se requiera (véase 16.1.7);

c) escalado del incidente, si así se requiere;

d) aseguramiento de que todos los implicados en las actividades de respuesta a incidentes son adecuadamente incorporados para realizar el correspondiente análisis posterior;

e) comunicación de la existencia del incidente de seguridad de la información o cualquier otro detalle relevante tanto para personas internas o externas o terceras entidades que se requiera deban tener conocimiento del mismo;

f) tratamiento de la debilidad o debilidades de seguridad de la información encontradas y que pudieran causar o contribuir al incidente;

g) una vez que el incidente ha sido satisfactoriamente tratado, el cierre y registro formales del mismo.

Tras el análisis del incidente debería tener lugar, en caso necesario, la identificación del origen del incidente.

Información adicional

El principal objetivo de la respuesta a un incidente es restaurar el “nivel normal de seguridad” y, entonces, iniciar la necesaria recuperación.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

Control

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

Guía de implantación

Deberían existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información a cuantificar y monitorizar. La información obtenida a partir de la evaluación de los incidentes de seguridad de la información debería utilizarse para identificar incidentes recurrentes o con un elevado alcance.

Información adicional

La evaluación de los incidentes de seguridad de la información puede sugerir la necesidad de mejorar o añadir controles para limitar la frecuencia, el daño y el coste de futuras apariciones, o para tenerlos en cuenta en el proceso de revisión (véase 5.1.2).

Prestando la debida atención a los aspectos de confidencialidad, los incidentes de seguridad de la información pueden utilizarse en los cursos de concienciación del usuario (véase 7.2.2) como ejemplos de lo que podría ocurrir, de cómo reaccionar ante esos incidentes y de cómo evitarlos en el futuro.

16.1.7 Recopilación de evidencias

Control

La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.

Guía de implantación

Deberían desarrollarse procedimientos internos para seguirse a la hora de recopilar y presentar pruebas con el fin de ejercer una acción disciplinaria y legal.

Por lo general, estos procedimientos de recogida de evidencias deberían proporcionar procesos de identificación, recogida, adquisición y preservación de las evidencias de acuerdo con los diferentes tipos de medios, dispositivos y condiciones de los mismos (por ejemplo, si están encendidos o apagados). Los procedimientos deberían tener en cuenta:

a) la cadena de custodia;

b) la integridad de la evidencia;

c) la protección de las personas;

d) las funciones o responsabilidades del personal implicado;

e) la competencia del personal;

f) la documentación;

g) el resumen.

Cuando esté disponible, se debería proporcionar una certificación u otros medios relevantes que acrediten la cualificación del personal y los instrumentos utilizados, de modo que refuercen el valor de la evidencia preservada.

Las evidencias forenses pueden trascender los límites de la organización o la jurisdicción. En estos casos, debería garantizarse que la organización está autorizada a recopilar la información requerida como prueba. También deberían tenerse en cuenta los requisitos de otras jurisdicciones con el fin de maximizar las oportunidades de admisión en todas las jurisdicciones competentes.

Información adicional

La identificación es el proceso relacionado con la búsqueda, el reconocimiento y la documentación de una posible evidencia. La recogida es el proceso de obtención de los ítems físicos que puede contener una posible evidencia. La adquisición es el proceso de creación de una copia de los datos en un determinado soporte. La preservación es el proceso de mantenimiento y custodia de la integridad y condición originales de la posible evidencia.

Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro de que se destruyan de forma intencional o accidental las evidencias necesarias antes de tomar conciencia de la gravedad del incidente. Es recomendable hacer uso de los servicios de un abogado o de la policía en las primeras fases de cualquier acción legal que se esté considerando, así como el asesorarse sobre las evidencias necesarias.

La Norma ISO/IEC 27037[24] proporciona directrices para la identificación, recogida, adquisición y preservación de las evidencias digitales.

17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

17.1 Continuidad de la seguridad de la información

Objetivo: La continuidad de la seguridad de la información debería formar parte de 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 necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Guía de implantación

La organización debería determinar si la continuidad de la seguridad de la información queda dentro del proceso de continuidad del negocio o dentro del proceso de gestión de la recuperación de desastres. Los requisitos de seguridad de información deberían determinarse al planificar la continuidad del negocio y la recuperación de desastres.

En ausencia de planes formales de continuidad del negocio y de recuperación de desastres, la gestión de la seguridad de la información debería asumir que los requisitos de seguridad de la información son los mismos tanto en condiciones adversas como en las condiciones normales de operación. Como alternativa, la organización puede realizar un análisis de impacto de negocio para los aspectos de seguridad de la información para determinar los requisitos de seguridad de la información aplicables en situaciones adversas.

Información adicional

Para reducir el tiempo y esfuerzo de un análisis de impacto de negocio 'adicional' para la seguridad de la información, se recomienda capturar estos aspectos durante el proceso de análisis de impacto en el negocio realizado durante la gestión de la continuidad o de la recuperación de desastres del negocio. Esto implica que los requisitos para la continuidad de la seguridad de la información se formulan explícitamente en los procesos de gestión de continuidad de negocio o de gestión de la recuperación de desastres.

Puede encontrarse información sobre la gestión de continuidad del negocio en las Normas ISO/IEC 27031[14], ISO 22313[9] e ISO 22301[8].

17.1.2 Implementar 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 requerido de continuidad de la seguridad de la información durante una situación adversa.

Guía de implantación

Una organización debería asegurar que:

a) existe una estructura de gestión adecuada y preparada para mitigar y responder a un evento disruptivo usando el personal con la autoridad, experiencia y competencia necesarias;

b) se ha nombrado al personal de respuesta al incidente y éste cuenta con la responsabilidad, autoridad y competencia necesarias para gestionar el incidente y mantener la seguridad de la información;

c) se han desarrollado y aprobado planes documentados y procedimientos de respuesta y recuperación que detallan como la organización gestionará un evento disruptivo y mantendrá la seguridad de su información en un nivel predeterminado, basado en los objetivos de continuidad de la seguridad de la información aprobados por dirección (véase 17.1.1).

De acuerdo con los requisitos de continuidad de seguridad de la información, la organización debería establecer, documentar, implantar y mantener:

a) controles de seguridad de la información en los procesos, procedimientos y sistemas y herramientas de soporte de continuidad del negocio o de recuperación de desastres;

b) procesos, procedimientos e implantación de cambios para mantener los controles existentes de seguridad de la información durante una situación adversa;

c) controles compensatorios para aquellos controles de seguridad de la información que no puedan mantenerse durante una situación adversa.

Información adicional

Pueden haberse definido procesos y procedimientos específicos en el contexto de la continuidad del negocio o de la recuperación de desastres. La información gestionada con éstos o con sistemas de información dedicados debería estar protegida. Por lo tanto, la organización debería involucrar a especialistas de seguridad de la información para establecer, implantar y mantener los procesos y procedimientos para la continuidad del negocio o la recuperación de desastres.

Los controles de seguridad de la información que sean implantados deberían continuar operativos durante una situación adversa. Si los controles de seguridad no hacen posible mantener la seguridad de la información, otros controles deberían ser establecidos e implantados 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 comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

Guía de implantación

Los cambios organizativos, técnicos, procedimentales y de proceso, tanto en el contexto operacional o de continuidad, pueden provocar cambios en los requisitos de continuidad de la seguridad de la información. En estos casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información deberían revisarse de acuerdo con éstos.

Las organizaciones deberían verificar su gestión de la continuidad de la seguridad de la información:

a) ejecutando y probando la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información asegurando que son consistentes con los objetivos de continuidad de seguridad de la información;

b) ejecutando y probando el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información asegurando que su rendimiento es consistente con los objetivos de continuidad de seguridad de la información;

c) revisando la validez y efectividad de las medidas para la continuidad de la seguridad de la información cuando cambien los sistemas de información, los procesos de seguridad de la información, los procedimientos y controles o los procesos y soluciones de gestión de continuidad de negocio y de recuperación de desastres.

Información adicional

La verificación de los controles de continuidad de seguridad del negocio es diferente de la prueba y verificación general de la seguridad de la información y debería realizarse de forma separada de la prueba de los cambios. Si es posible, es preferible integrar la verificación de los controles de seguridad de la información con las pruebas de continuidad de negocio o de recuperación de desastres de la organización.

17.2 Redundancias

Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.

17.2.1 Disponibilidad de los recursos de tratamiento de la información

Control

Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

Guía de implantación

Las organizaciones deberían identificar los requisitos de disponibilidad para los sistemas de información. Cuando la disponibilidad no pueda garantizarse usando la arquitectura de sistemas existentes, deberían considerarse componentes o arquitecturas redundantes.

Cuando sea aplicable, los sistemas de información redundantes deberían probarse para asegurar que la conmutación de un componente a otro funciona como se espera.

Información adicional

La implantación de redundancias puede introducir riesgos a la integridad o confidencialidad de la información y a los sistemas de información que deberían ser considerados al diseñar los sistemas de información.

18 Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.

Guía de implantación

Deberían también definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir estos requisitos.

Los directivos o responsables deberían identificar toda la legislación aplicable a sus organizaciones para cumplir con los requisitos de su tipo de negocio. Si la organización tiene actividades de negocio en otros países, los directivos o responsables deberían considerar el cumplimiento en todos los países relevantes.

18.1.2 Derechos de propiedad intelectual (DPI)

Control

Deberían implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Guía de implantación

Deberían tenerse en cuenta las siguientes directrices para proteger cualquier material que pueda ser considerado propiedad intelectual:

a) publicar una política para el cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos software y de los de información;

b) adquirir software únicamente a través de las fuentes conocidas y de confianza para garantizar que no se infringen los derechos de autor;

c) mantener el conocimiento de las políticas de protección de los derechos de propiedad intelectual y notificar la intención de aplicar medidas disciplinarias a cualquier miembro del personal que quebrante dichas políticas;

d) mantener registros adecuados de los activos e identificar todos los activos que requieran la protección de los derechos de propiedad intelectual;

e) mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.;

f) implementar controles para garantizar que no se excede el número máximo de usuarios permitidos por la licencia;

g) llevar a cabo comprobaciones de que sólo se instala software autorizado y productos licenciados;

h) disponer de una política para mantener las condiciones de las licencias en forma adecuada;

i) disponer de una política para eliminar el software o para transferirlo a un tercero cuando cese su uso;

j) cumplir las condiciones contractuales del software y de la información que se obtenga de redes públicas;

k) no duplicar ni convertir a otro formato y no extraer de grabaciones comerciales (película, audio) nada más que lo que permita la ley de derechos de autor;

l) no copiar parcial o totalmente libros, artículos, informes u otros documentos salvo lo que permita la ley de derechos de autor.

Información adicional

Los derechos de propiedad intelectual incluyen los derechos de autor sobre software o documentos, diseños, marcas comerciales, patentes y licencias sobre el código fuente.

Los productos software propietarios se suelen suministrar con un contrato de licencia que especifica las condiciones de la misma, por ejemplo, limitando el uso de los productos a unas máquinas específicas o limitando las copias exclusivamente a las de respaldo. Debería comunicarse al personal la importancia de los derechos de propiedad intelectual para el software desarrollado por la organización y concienciar sobre este tema.

Los requisitos legales, reglamentarios y contractuales pueden plantear restricciones a la copia del material propietario. En particular, pueden exigir que sólo pueda utilizarse material desarrollado por la organización, que cuente con licencia o que haya sido suministrado por el desarrollador a la organización. La infracción de los derechos de autor puede desembocar en acciones legales que pueden incluir multas y procedimientos penales.

18.1.3 Protección de los registros de la organización

Control

Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

Guía de implantación

Debería considerarse la clasificación de los registros de acuerdo con el esquema establecido en la organización al decidir su protección. Los registros deberían categorizarse en tipos, por ejemplo, registros contables, registros de la base de datos, registros de transacciones, registros de auditoría y procedimientos operacionales, cada uno de ellos con detalles sobre los periodos de retención y los medios de almacenamiento permitidos, por ejemplo, papel, microfichas, magnéticos, ópticos. Debería almacenarse también cualquier clave criptográfica y programa asociado con archivos cifrados o firmas electrónicas (véase el capítulo 10) para permitir descifrar los registros durante el periodo de tiempo que éstos deberían ser retenidos.

Debería considerarse la posibilidad que los medios usados para el almacenamiento de los registros se deterioren. Los procedimientos para el almacenamiento y manipulación deberían estar implementados de acuerdo con las recomendaciones del fabricante.

Si se escogen soportes electrónicos de almacenamiento, deberían establecerse procedimientos que aseguren el acceso a los datos (tanto la legibilidad del soporte como del formato) durante el periodo de retención con el fin de proteger contra la pérdida causada por futuros cambios de la tecnología.

Deberían escogerse los sistemas de almacenamiento de datos teniendo en cuenta que los datos deberían ser recuperados en plazo y formato aceptables dependiendo de los requisitos a cumplir.

El sistema de almacenamiento y manipulación debería garantizar una clara identificación de los registros y de sus periodos de retención según defina la legislación y reglamentación nacional o regional que fuera aplicable. El sistema debería permitir la destrucción adecuada de los registros tras ese periodo si dejan de ser necesarios para la organización.

Para cumplir los objetivos de salvaguarda de esos registros, la organización debería seguir los siguientes pasos:

a) debería publicar directrices sobre la retención, almacenamiento, manipulación y eliminación de registros e información;

b) debería prepararse un calendario de retención que identifique los registros y el periodo de tiempo que deberían conservarse;

c) debería mantenerse un inventario de fuentes de información clave.

Información adicional

Algunos registros pueden necesitar ser retenidos de forma segura para cumplir con los requisitos legales, reglamentarios o contractuales además de dar soporte a las actividades esenciales del negocio. Los ejemplos incluyen registros que pueden ser requeridos como evidencia de que la organización opera de acuerdo con las reglas legales o reglamentarias, para asegurar la defensa ante demandas civiles o penales o para confirmar el estado financiero de la organización a accionistas, terceros y auditores. Las leyes o reglamentos nacionales pueden establecer el plazo y el contenido de la información a retener.

Puede encontrarse más información sobre la gestión de los registros organizacionales en la Norma ISO 15489-1[5].

18.1.4 Protección y privacidad de la información de carácter personal

Control

Debería garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Guía de implantación

Debería desarrollarse e implantarse una política de privacidad y protección de la información de carácter personal. Dicha política debería comunicarse a todas las personas involucradas en el tratamiento de la información de carácter personal.

El cumplimiento con esta política y la legislación y reglamentos aplicables sobre la privacidad de las personas y la protección de los datos de carácter personal requiere una estructura apropiada para su gestión y control. A menudo, la mejor manera es nombrar un responsable de protección de datos que debería orientar a los directivos, responsables, usuarios y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos a seguir. La responsabilidad para el tratamiento de la información de carácter personal y la garantía de que se conocen los principios de privacidad debería estar de acuerdo con la legislación y reglamentación aplicable. Deberían implantarse las medidas técnicas y organizativas apropiadas para proteger la información de carácter personal.

Información adicional

La Norma ISO/IEC 29100[25] contiene un marco de alto nivel para la protección de la información de carácter personal en los sistemas de información y comunicación. Varios países cuentan con legislación que define los controles a aplicar a la recogida, proceso y transmisión de la información de carácter personal (normalmente la información sobre personas vivas que puedan ser identificadas a partir de dicha información). Dependiendo de la legislación nacional, estos controles pueden imponer obligaciones en la recogida, tratamiento y diseminación de la información de carácter personal y también restringir la capacidad de transferir ésta a otros países.

18.1.5 Regulación de los controles criptográficos

Control

Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

Guía de implantación

Para el cumplimiento de los acuerdos, legislación y reglamentación aplicables deberían considerarse los puntos siguientes:

a) las restricciones en la importación o exportación de hardware y software que realice funciones criptográficas;

b) las restricciones en la importación o exportación de hardware y software diseñado para tener funciones criptográficas añadidas;

c) las restricciones al uso del cifrado;

d) los métodos de acceso obligatorio o discrecional para las autoridades de los países a la información cifrada con hardware y software que proporcione confidencialidad al contenido.

Debería contarse con consejo legal para asegurar el cumplimiento con la legislación y reglamentación aplicable. También en el caso de transferencia de información cifrada o controles criptográficos entre países.

18.2 Revisiones de la seguridad de la información

Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

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 implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

Guía de implantación

La dirección debería encargar la revisión independiente. Dicha revisión es necesaria para asegurar la adecuación continua y la efectividad de la forma en la que la organización gestiona la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del enfoque establecido, incluyendo la política y los objetivos de control.

Esta revisión debería ser realizada por individuos independientes al área revisada, por ejemplo, ser realizada por la función de auditoría interna, un director independiente o contratada a una organización externa que realice dichas revisiones. Los revisores deberían contar con los conocimientos y experiencia necesaria.

Los resultados de la revisión independiente deberían quedar debidamente registrados y ser presentados a la dirección que encargó la revisión. Estos registros deberían ser mantenidos.

Si la revisión independiente identifica que el enfoque de la organización para la gestión de la seguridad de la información y su implantación es inadecuada, por ejemplo, si no se cumplen los objetivos documentados y los requisitos o bien éstos no cumplen con lo establecido para la seguridad de la información en las políticas de seguridad de la información (véase 5.1.1), la dirección debería considerar acciones correctivas.

Información adicional

Las Normas ISO/IEC 27007[12], "*Information technology. Security techniques. guidelines for information security management systems auditing*" e ISO/IEC 27008[13], "*Information technology. Security techniques. Guidelines for auditors on information security controls*" también proporcionan directrices adicionales para realizar una revisión independiente.

18.2.2 Cumplimiento de las políticas y normas de seguridad

Control

Los directivos deberían asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

Guía de implantación

Los directivos o responsables deberían determinar cómo revisar los requisitos de seguridad de la información definidos en las políticas, normas y otra reglamentación a cumplir. Se deberían considerar las herramientas automáticas de medida y presentación para una revisión periódica eficiente.

Si como resultado de la revisión se identifica algún incumplimiento, los directivos o responsables deberían:

a) identificar las causas del incumplimiento;

b) evaluar las acciones necesarias para el cumplimiento;

c) implementar las acciones correctivas necesarias;

d) revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

Los resultados de las revisiones y de las acciones correctivas realizadas por los directores deberían ser registradas y los registros deberían ser mantenidos. Los directivos o responsables deberían informar de los resultados a las personas que realizaron las revisiones independientes (véase 18.2.1) cuando dicha revisión se realice en su área de responsabilidad.

Información adicional

La monitorización operativa del uso del sistema se trata en el apartado 12.4.

18.2.3 Comprobación del cumplimiento técnico

Control

Debería comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Guía de implantación

El cumplimiento técnico debería revisarse preferiblemente con la ayuda de herramientas automáticas que generen informes técnicos que posteriormente interprete un especialista técnico. Alternativamente, un ingeniero de sistemas podría realizar revisiones manuales (apoyadas, si fuera necesario, por herramientas software).

Debería tenerse cuidado cuando se realicen pruebas de intrusión o evaluación de vulnerabilidades, puesto que podrían comprometer la seguridad del sistema. Dichas pruebas deberían planificarse, documentarse y ser repetibles.

Toda revisión de cumplimiento técnico debería tan solo realizarse por personal competente y autorizado o bajo la supervisión de dichas personas.

Información adicional

Las revisiones de cumplimiento técnico implican el examen de los sistemas en producción o en explotación para asegurar que los controles hardware y software han sido correctamente implantados. Este tipo de revisión de cumplimiento requiere conocimientos técnicos especializados.

Las revisiones de cumplimiento también cubren, por ejemplo, las pruebas de intrusión y la evaluación de vulnerabilidades que pueden ser realizadas por expertos independientes contratados específicamente para ello. Éstas pueden ser útiles para detectar las vulnerabilidades del sistema y la efectividad de los controles para prevenir el acceso no autorizado debido a esas vulnerabilidades.

Las pruebas de intrusión o la evaluación de vulnerabilidades proporcionan una imagen fija de un sistema en un estado y tiempo determinado. Esta imagen tan sólo refleja la parte del sistema probado realmente durante el(los) intento(s) de penetración. Las pruebas de intrusión y la evaluación de vulnerabilidades no reemplazan a la evaluación de riesgos.

La Norma ISO/IEC TR 27008[13] proporciona directrices específicas para las 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] ISO 15489-1, *Information and documentation. Records management. Part 1: General.*

[6] ISO/IEC 20000-1, *Information technology. Service management. Part 1: Service management system requirements.*

[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] ISO/IEC 27001, *Information technology. Security techniques. Information security management systems. Requirements.*

[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.*

1) La Norma ISO/IEC 20000-2:2005 ha sido anulada y sustituida por la Norma ISO/IEC 20000-2:2012 Tecnología de la información. Gestión del servicio. Parte 2: Directrices para la aplicación del Sistema de Gestión del Servicio (SGS).

[17] ISO/IEC 27033-3, *Information technology. Security techniques. Network security. Part 3: Reference networking scenarios. Threats, design techniques and control issues.*

[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] ISO/IEC 27035, *Information technology. Security techniques. Information security incident management.*

[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] ISO 31000, *Risk management. Principles and guidelines.*

Anexo A (Informativo)

Nota nacional

Es importante señalar que el presente documento, al tener el carácter de norma nacional idéntica a la Norma ISO/IEC 27002:2013, para un lector que se limite a considerar capítulos o apartados de manera aislada, como por ejemplo, el capítulo 8, podría tener la impresión que la norma incurre puntualmente en aspectos que pueden ser objeto de conflicto con la legislación aplicable en el marco español.

Pero si la norma se contempla en su totalidad, se verá que sí tiene en cuenta los mencionados aspectos, indicando el debido cumplimiento de la legislación aplicable en cada estado.

Para información relacionada con el desarrollo de las normas contacte con:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR Internacional, SAU
Tel.: 914 326 000
normas@aenor.com
www.aenor.com