norma española

UNE-ISO/IEC 27001

Noviembre 2014

TÍTULO

Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de Seguridad de la Información (SGSI)

Requisitos

Information technology. Security techniques. Information security management systems. Requirements.

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Exigences.

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO/IEC 27001:2013.

OBSERVACIONES

ANTECEDENTES

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

Editada e impresa por AENOR
Depósito legal: M 32359:2014

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

30 Páginas

Índice

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 tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como norma internacional requiere la aprobación por al menos el 75% de los organismos miembros que emiten voto.

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.

La Norma ISO/IEC 27001 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1 *Tecnología de la Información*, SC 27 *Técnicas de seguridad.*

Esta segunda edición anula y sustituye a la primera edición (Norma ISO 27001:2005) que ha sido revisada técnicamente.

0 Introducción

0.1 Generalidades

Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información por una organización está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Lo previsible es que todos estos factores condicionantes cambien con el tiempo.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.

Es importante que el sistema de gestión de seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la implementación del sistema de gestión de seguridad de la información se ajuste a las necesidades de la organización.

Esta norma internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad.

El orden en que esta norma internacional presenta los requisitos no es reflejo de su importancia ni implica el orden en el cual deben implementarse. Los diferentes elementos de cada listado se enumeran sólo a título de referencia.

La Norma ISO/IEC 27000 describe la visión de conjunto y el vocabulario de los sistemas de gestión de seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de seguridad de la información (incluyendo las Normas ISO/IEC 27003 [2], ISO/IEC 27004 [3] e ISO/IEC 27005 [4]), junto con los términos y definiciones relacionados.

0.2 Compatibilidad con otras normas de sistema de gestión

Esta norma internacional emplea la estructura de alto nivel, texto esencial idéntico, términos y definiciones esenciales comunes contenidos en el anexo SL de la Parte 1 de las Directivas ISO/IEC, Suplemento ISO consolidado y por lo tanto mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el anexo SL.

Este enfoque común definido en el anexo SL será útil para aquellas organizaciones que deciden implantar un sistema de gestión que cumpla con los requisitos de dos o más normas de sistemas de gestión

1 Objeto y campo de aplicación

Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza. No se acepta la declaración de conformidad con respecto a esta norma internacional habiendo excluido alguno de los requisitos especificados en los capítulos 4 al 10.

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 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

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

NOTA La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado 5.3 de la Norma ISO 31000:2009 [5].

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información; y

b) los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, así como obligaciones contractuales.

4.3 Determinación del alcance del sistema de gestión de seguridad de la información

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

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el apartado 4.1;

b) los requisitos referidos en el apartado 4.2;

c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar de manera continúa un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional.

5 Liderazgo

5.1 Liderazgo y compromiso

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

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

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

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

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

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

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

g) promoviendo la mejora continua; y

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

5.2 Política

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

a) sea adecuada al propósito de la organización;

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

c) incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e

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

La política de seguridad de la información debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización; y

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

5.3 Roles, responsabilidades y autoridades en la organización

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

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de seguridad de la información es conforme con los requisitos de esta norma internacional; e

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

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

6 Planificación

6.1 Acciones para tratar los riesgos y oportunidades

6.1.1 Consideraciones generales

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

a) asegurar que el sistema de gestión de seguridad de la información pueda conseguir sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

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

e) la manera de:

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

2) evaluar la eficacia de estas acciones.

6.1.2 Apreciación de riesgos de seguridad de la información

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

a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:

1) los criterios de aceptación de riesgo, y

2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información,

b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;

c) identifique los riesgos de seguridad de la información:

1) llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de seguridad de la información,

2) identificando a los dueños de los riesgos;

d) analice los riesgos de seguridad de la información:

   1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,

   2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en 6.1.2 c) 1),

   3) determinando los niveles de riesgo,

e) evalúe los riesgos de seguridad de la información:

   1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),

   2) priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

6.1.3 Tratamiento de los riesgos de seguridad de la información

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

a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;

b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

   NOTA Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

c) comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

   NOTA 1 El anexo A contiene una amplia lista de objetivos de control y controles. Se indica a los usuarios de esta norma internacional que se dirijan al anexo A para asegurar que no se pasan por alto controles necesarios.

   NOTA 2 Los objetivos de control se incluyen implícitamente en los controles seleccionados. Los objetivos de control y los controles enumerados en el anexo A no son exhaustivos, por lo que pueden ser necesarios objetivos de control y controles adicionales.

d) elaborar una "Declaración de Aplicabilidad" que contenga los controles necesarios (véanse los puntos 6.1.3 b) y c)) y la justificación de las inclusiones, estén implementadas o no, y la justificación de las exclusiones de los controles del anexo A;

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

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

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en esta norma internacional se alinean con los principios y directrices genéricas definidos en la Norma ISO 31000 [5].

6.2 Objetivos de seguridad de la información y planificación para su consecución

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

Los objetivos de seguridad de la información deben:

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

b) ser medibles (si es posible);

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

d) ser comunicados; y

e) ser actualizados, según sea apropiado.

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

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:

f) lo que se va a hacer;

g) qué recursos se requerirán;

h) quién será responsable;

i) cuándo se finalizará; y

j) cómo se evaluarán los resultados.

7 Soporte

7.1 Recursos

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

7.2 Competencia

La organización debe:

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

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

c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y

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

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

7.3 Concienciación

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

a) la política de la seguridad de la información;

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

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

7.4 Comunicación

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

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar;

e) los procesos por los que debe efectuarse la comunicación.

7.5 Información documentada

7.5.1 Consideraciones generales

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

a) la información documentada requerida por esta norma internacional;

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

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

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

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

3) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

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

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

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

7.5.3 Control de la información documentada

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

a) esté disponible y preparada para su uso, dónde y cuándo se necesite;

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

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

c) distribución, acceso, recuperación y uso;

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

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

f) retención y disposición.

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

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

8 Operación

8.1 Planificación y control operacional

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

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

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

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

8.2 Apreciación de los riesgos de seguridad de información

La organización debe efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a).

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

8.3 Tratamiento de los riesgos de seguridad de información

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

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

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

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

La organización debe determinar:

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

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

NOTA Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

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

d) quién debe hacer el seguimiento y la medición;

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

f) quién debe analizar y evaluar esos resultados.

La organización debe conservar la información documentada adecuada como evidencia de los resultados.

9.2 Auditoría interna

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

a) cumple con:

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

2) los requisitos de esta norma internacional,

b) está implementado y mantenido de manera eficaz.

La organización debe:

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

d) para cada auditoría, definir sus criterios y su alcance;

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

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

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

9.3 Revisión por la dirección

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

La revisión por la dirección debe incluir consideraciones sobre:

a) el estado de las acciones desde anteriores revisiones por la dirección;

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

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

   1) no conformidades y acciones correctivas,

   2) seguimiento y resultados de las mediciones,

   3) resultados de auditoría, y

   4) el cumplimiento de los objetivos de seguridad de la información,

d) los comentarios provenientes de las partes interesadas;

e) los resultados de la apreciación del riesgo y el estado del plan de tratamiento de riesgos; y

f) las oportunidades de mejora continua.

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

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

10 Mejora

10.1 No conformidad y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

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

   1) llevar a cabo acciones para controlarla y corregirla, y

   2) hacer frente a las consecuencias,

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

   1) la revisión de la no conformidad,

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

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

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas llevadas a cabo; y

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

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

La organización debe conservar información documentada, como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo; y

g) los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar de manera continúa la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información.

Anexo A (Normativo)

Objetivos de control y controles de referencia

Los objetivos de control y controles que se enumeran en la tabla A.1 se corresponden directamente con los que figuran en la Norma ISO/IEC 27002:2013 [1], capítulos 5 a 18, y deben ser empleados en el contexto del apartado 6.1.3.

Tabla A.1 – Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Directrices de gestión de la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
A.6 Organización de la seguridad de la información		
A.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.		
A.6.1.1	Roles y responsabilidades en seguridad de la información	*Control* Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de tareas	*Control* Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

A.6.2 Los dispositivos móviles y el teletrabajo		
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
A.7 Seguridad relativa a los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Para asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.		
A.7.1.1	Investigación de antecedentes	*Control* La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	*Control* La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas, deben 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.
A.7.2.3	Proceso disciplinario	*Control* Debe 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.

A.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.		
A.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 deben definir, comunicar al empleado o contratista y se deben cumplir.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	*Control* Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	*Control* Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben 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.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.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.		
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.2.3	Manipulado de la información	*Control* Debe 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.

A.8.3 Manipulación de los soportes		
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.		
A.8.3.1	Gestión de soportes extraíbles	*Control* Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	*Control* Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	*Control* Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
A.9 Control de acceso		
A.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.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	*Control* Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A.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.		
A.9.2.1	Registro y baja de usuario	*Control* Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	*Control* Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	*Control* La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	*Control* La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.

A.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 deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información secreta de autenticación	*Control* Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.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 debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.4	Uso de utilidades con privilegios del sistema	*Control* Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.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.		
A.10.1.1	Política de uso de los controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

A.11 Seguridad física y del entorno		
A.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.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.
A.11.1.2	Controles físicos de entrada	*Control* Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, despachos y recursos	*Control* Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A.11.1.4	Protección contra las amenazas externas y ambientales	*Control* Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A.11.1.5	El trabajo en áreas seguras	*Control* Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
A.11.1.6	Áreas de carga y descarga	*Control* Deben 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.
A.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.		
A.11.2.1	Emplazamiento y protección de equipos	*Control* Los equipos deben 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.
A.11.2.2	Instalaciones de suministro	*Control* Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
A.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 debe estar protegido frente a interceptaciones, interferencias o daños.

A.11.2.4	Mantenimiento de los equipos	*Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A.11.2.5	Retirada de materiales propiedad de la empresa	*Control* Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	*Control* Deben 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,.
A.11.2.7	Reutilización o eliminación segura de equipos	*Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	*Control* Debe 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.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
A.12.1.1	Documentación de procedimientos de los operación	*Control* Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
A.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 deben ser controlados.
A.12.1.3	Gestión de capacidades	*Control* Se debe 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.
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	*Control* Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

A.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.		
A.12.2.1	Controles contra el código malicioso	*Control* Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3 Copias de seguridad		
Objetivo: Evitar la pérdida de datos		
A.12.3.1	Copias de seguridad de la información	*Control* Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.4 Registros y supervisión		
Objetivo: Registrar eventos y generar evidencias.		
A.12.4.1	Registro de eventos	*Control* Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	*Control* Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de administración y operación	*Control* Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
A.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, deben estar sincronizados con una única fuente precisa y acordada de tiempo.
A.12.5 Control del software en explotación		
Objetivo: Asegurar la integridad del software en explotación.		
A.12.5.1	Instalación del software en explotación	*Control* Se deben implementar procedimientos para controlar la instalación del software en explotación.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe 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.

A.12.6.2	Restricción en la instalación de software	*Control* Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre la auditoria de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.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 deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.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.		
A.13.1.1	Controles de red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A.13.2 Intercambio de información		
Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de intercambio de información	*Control* Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
A.13.2.2	Acuerdos de intercambio de información	*Control* Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
A.13.2.3	Mensajería electrónica	*Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no revelación	*Control* Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.14.1 Requisitos de seguridad en 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.		
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	*Control* La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	*Control* La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.
A.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 sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
A.14.2.2	Procedimiento de control de cambios en sistemas	*Control* La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.
A.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 deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.
A.14.2.4	Restricciones a los cambios en los paquetes de software	*Control* Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.
A.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben 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.

A.14.2.7	Externalización del desarrollo de software	*Control* El desarrollo de software externalizado debe ser supervisado y controlado por la organización.
A.14.2.8	Pruebas funcionales de seguridad de sistemas	*Control* Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	*Control* Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos de prueba		
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
A.15 Relación con proveedores		
A.15.1 Seguridad en las relaciones con proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información 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 deben acordarse con el proveedor y quedar documentados.
A.15.1.2	Requisitos de seguridad en contratos con terceros	*Control* Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	*Control* Los acuerdos con proveedores deben 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.
A.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		
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	*Control* Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor

A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	*Control* Se deben 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.
A.16 Gestión de incidentes de seguridad de la información		
A.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.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A.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 deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.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 debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	*Control* La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de continuidad de negocio de la organización.		

A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementar la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias.		
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.		
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	*Control* Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A.18 Cumplimiento		
A.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.		
A.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, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.
A.18.1.2	Derechos de propiedad intelectual (DPI)	*Control* Deben 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.
A.18.1.3	Protección de los registros de la organización	*Control* Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.
A.18.1.4	Protección y privacidad de la información de carácter personal	*Control* Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.
A.18.1.5	Regulación de los controles criptográficos	*Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

A.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.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	*Control* Los directivos deben asegurarse de 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
A.18.2.3	Comprobación del cumplimiento técnico	*Control* Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Bibliografía

[1] ISO/IEC 27002:2013, *Information technology. Security Techniques. Code of practice for information security controls.*

[2] ISO/IEC 27003, *Information technology. Security techniques. Information security management system implementation guidance.*

[3] ISO/IEC 27004, *Information technology. Security techniques. Information security management. Measurement.*

[4] ISO/IEC 27005, *Information technology. Security techniques. Information security risk management.*

[5] ISO 31000:2009, *Risk management. Principles and guidelines.*

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

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032