iram-iso-iec-27001

31 pag.

NORMA ARGENTINA

IRAM-ISO/IEC 27001*

Segunda edición
2015-09-03

Tecnología de la información

Técnicas de seguridad

Sistemas de gestión de la seguridad de la información

Requisitos

(ISO/IEC 27001:2013, IDT)

Information technology
Security techniques
Information security management systems
Requirements

* **Corresponde a la revisión de la primera edición, a la que esta segunda edición reemplaza.**

Referencia Numérica:
IRAM-ISO/IEC 27001:2015

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

Corresponde a la revisión de la primera edición (2007), a la que esta segunda edición reemplaza.

Esta norma es una adopción idéntica (IDT) de la norma ISO/IEC 27001:2013 - *Information technology - Security techniques - Information security management systems - Requirements.*

Solo se han realizado los cambios editoriales siguientes:

Se agregó un anexo informativo con la bibliografía considerada y otro donde se indican los organismos de estudio de la norma.

Prefacio ISO

La International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) constituyen un 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 tratar temas particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Las normas internacionales se elaboran de acuerdo a las reglas dadas en la Directiva ISO/IEC, parte 2.

La tarea principal del comité técnico conjunto es la de preparar normas internacionales. Los proyectos de normas internacionales adoptadas por el comité técnico conjunto son circulados a los organismos nacionales y sometidos a votación. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos nacionales.

Es importante señalar la posibilidad de que algunos elementos de esta norma internacional pueden estar sujetos a derechos de patente. ISO e IEC no son responsables de la identificación de alguno o todos de esos derechos de patentes.

La norma ISO/IEC 27001 fue preparada por el comité técnico conjunto ISO/IEC JTC1, *Information Technology*, subcomité SC 27, *IT Security Techniques*.

Esta segunda edición anula y reemplaza a la primera edición (ISO/IEC 27001:2005), la cual ha sido revisada técnicamente.

Índice

Tecnología de la información

Técnicas de seguridad

Sistemas de gestión de la seguridad de la información

Requisitos

0 INTRODUCCIÓN

0.1 Generalidades

Esta norma se ha elaborado para brindar los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI es una decisión estratégica para una organización. El establecimiento y la implementación del SGSI de una organización están influenciados por sus necesidades y objetivos, los requisitos de seguridad, los procesos organizacionales empleados y el tamaño y la estructura de la organización. Se espera que estos factores cambien a lo largo del tiempo.

El SGSI preserva la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y da confianza a las partes interesadas acerca de la gestión adecuada de los riesgos.

Es importante que el SGSI sea parte de los procesos de la organización y de la estructura general de gestión y se integre a éstos, y que la seguridad de la información se considere al diseñar procesos, sistemas de información y controles. Se espera que la implementación de un SGSI escale de acuerdo con las necesidades de la organización.

Esta norma la pueden usar, tanto las partes internas como externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad de la información.

El orden en que se presentan los requisitos en esta norma no refleja su importancia ni implica un orden en el cual se deban implementar. Los elementos de una lista se enumeran únicamente para permitir su referencia.

La ISO/IEC 27000 describe de manera general y provee el vocabulario para los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas del SGSI (incluyendo la ISO/IEC 27003, la IRAM-ISO/IEC 27004 y la IRAM-NM-ISO/IEC 27005), junto con los términos y definiciones relacionados.

0.2 Compatibilidad con otros sistemas de gestión

Esta norma aplica la estructura de alto nivel, los títulos idénticos de apartados, el texto idéntico, los términos comunes y las definiciones esenciales establecidos en el Anexo SL de la Directiva ISO/IEC, Parte 1, *Consolidated ISO Supplement*, y, por lo tanto, es compatible con otras normas de sistemas de gestión que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL es de utilidad para aquellas organizaciones que eligen operar un único 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 especifica los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un SGSI dentro del contexto la organización. Esta norma también incluye los requisitos para la evaluación y el tratamiento de los riesgos a la seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y la intención es que sean aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Cuando una organización declara conformidad con esta norma, no puede excluir ninguno de los requisitos especificados en los capítulos 4 a 10.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, significa que se debe aplicar dicha edición. En caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

*ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary.

*ISO/IEC 27002:2013 - Information technology - Security techniques - Information security management systems - Requirements.

* Hasta tanto se estudien las normas IRAM correspondientes se toman las normas internacionales mencionadas como documentos para consulta.

3 TÉRMINOS Y DEFINICIONES

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

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y su contexto

La organización debe determinar las cuestiones internas y externas que son pertinentes a su propósito y que afectan su capacidad para alcanzar los resultados previstos de su SGSI.

NOTA. La determinación de estas cuestiones se refiere al establecimiento del contexto interno y externo de la organización considerado en 5.3 de la IRAM-ISO 31000:2015.

4.2 Comprensión de las necesidades y las expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son pertinentes al SGSI;

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

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

4.3 Determinación del alcance del SGSI

La organización debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

a) las cuestiones internas y externas mencionadas en 4.1;

b) los requisitos mencionados en 4.2;

c) las interfaces y las dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de la seguridad de la información (SGSI)

La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, de acuerdo con los requisitos de esta norma.

5 LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI:

a) asegurando el establecimiento de la política y los objetivos de la seguridad de la información y su compatibilidad con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del SGSI con los procesos de la organización;

c) asegurando la disponibilidad de los recursos necesarios para el sistema de gestión de la seguridad de la información;

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

e) asegurando que el SGSI logre los resultados previstos;

f) dirigiendo y apoyando personas, para contribuir a la eficacia del SGSI;

g) promoviendo la mejora continua;

h) apoyando otros roles pertinentes de la dirección para que demuestren 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 apropiada al propósito de la organización;

b) incluya los objetivos de seguridad de la información (ver 6.2) o proporcione un marco para establecer los objetivos de seguridad de la información;

c) incluya el compromiso de cumplir los requisitos pertinentes relativos a la seguridad de la información;

d) incluya el compromiso de mejora continua del SGSI.

La política de seguridad de la información debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización;

g) estar disponible para las partes interesadas, cuando corresponda.

5.3 Roles, responsabilidades y autoridades en la organización

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

La alta dirección debe asignar la responsabilidad y la autoridad para:

a) asegurar que el SGSI es conforme con los requisitos de esta norma;

b) informar a la alta dirección acerca del desempeño del SGSI.

NOTA. La alta dirección también puede asignar las responsabilidades y las autoridades para informar acerca del desempeño del SGSI dentro de la organización.

6 PLANIFICACIÓN

6.1 Acciones para tratar los riesgos y las oportunidades

6.1.1 Generalidades

Al planificar el SGSI, la organización debe considerar las cuestiones mencionadas en 4.1 y los requisitos mencionados en 4.2 y determinar los riesgos y las oportunidades que deben tratarse para:

a) asegurar que el SGSI pueda lograr el o los resultados previstos;

b) prevenir o reducir los efectos no deseados;

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades;

e) cómo

1) integrar e implementar las acciones dentro de los procesos de su SGSI;

2) evaluar la eficacia de estas acciones.

6.1.2 Evaluación del riesgo respecto a la seguridad de la información

La organización debe definir y aplicar un proceso de evaluación del riesgo a la seguridad de la información que:

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

1) los criterios de aceptación del riesgo;

2) los criterios para la realización de la evaluación del riesgo a la seguridad de la información;

b) asegure que evaluaciones reiteradas del riesgo a la seguridad de la información produzcan resultados coherentes, válidos y comparables;

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

1) aplique el proceso de evaluación del riesgo a la seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI;

2) identifique los propietarios de los riesgos;

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

1) evalúe las consecuencias potenciales que podrían resultar si se materializaran los riesgos identificados en 6.1.2 c) 1);

2) evalúe la probabilidad realista de ocurrencia de los riesgos identificados en 6.1.2 c) 1);

3) determine los niveles de riesgo;

e) valore los riesgos a la seguridad de la información;

1) compare los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a);

2) priorice los riesgos analizados para su tratamiento.

La organización debe conservar información documentada sobre el proceso de evaluación del riesgo a la seguridad de la información.

6.1.3 Tratamiento del riesgo a la seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento del riesgo a la seguridad de la información para:

a) seleccionar las opciones apropiadas de tratamiento del riesgo a la seguridad de la información, teniendo en cuenta los resultados de la evaluación del riesgo;

b) determinar todos los controles que sean necesarios para implementar la o las opciones de tratamiento del riesgo seleccionadas;

NOTA. Las organizaciones pueden diseñar los controles tal como se requiere o identificarlos a partir de alguna fuente.

c) comparar los controles determinados en 6.1.3 b) con los indicados en el anexo A y verificar que no se hayan omitido controles necesarios;

NOTA 1. El anexo A contiene una lista amplia de objetivos de control y controles. Los usuarios de esta norma deben dirigirse al anexo A para asegurarse que no hayan omitido algún control necesario.

NOTA 2. Los objetivos de control están incluidos implícitamente en los controles seleccionados. Los objetivos de control y los controles indicados en el anexo A no son exhaustivos y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) y c)) y la justificación de inclusiones, estén implementados o no, y la justificación de las exclusiones de controles del anexo A;

e) formular un plan de tratamiento del riesgo a la seguridad de la información;

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

La organización debe conservar información documentada sobre el proceso de tratamiento del riesgo a la seguridad de la información.

NOTA. El proceso de evaluación y tratamiento del riesgo a la seguridad de la información de esta norma se alinea con los principios y las guías generales, indicados en la IRAM-ISO 31000.

6.2 Objetivos de seguridad de la información y planificación para lograrlos

La organización debe establecer objetivos de seguridad de la información a 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 (de ser posible);

c) tener en cuenta los requisitos de seguridad de la información pertinentes y los resultados de la evaluación y el tratamiento del riesgo;

d) ser comunicados;

e) ser actualizados como corresponda.

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

Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

f) qué se va a hacer;

g) qué recursos se van a necesitar;

h) quién va a ser responsable;

i) cuándo se va a completar;

j) cómo se van a evaluar los resultados.

7 SOPORTE

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI.

7.2 Competencia

La organización debe:

a) determinar la competencia necesaria de la o las personas bajo su control que realicen trabajo que afecte el desempeño de la organización en cuanto a la seguridad de la información;

b) asegurar que estas personas sean competentes en función de la educación, la capacitación o la experiencia apropiadas;

c) cuando corresponda, realizar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones realizadas;

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

NOTA. Las acciones pertinentes pueden incluir, por ejemplo: proporcionar capacitación, tutores o reasignar empleados actuales; o emplear o contratar personas competentes.

7.3 Concientización

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

a) la política de seguridad de la información;

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

c) las implicancias de no cumplir con los requisitos del SGSI.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI, incluyendo:

a) qué comunicar;

b) cuándo comunicar;

c) con quién comunicarse;

d) quién debe comunicar;

e) los procesos mediante los cuales se va a realizar la comunicación.

7.5 Información documentada

7.5.1 Generalidades

El SGSI de la organización debe incluir:

a) la información documentada requerida por esta norma;

b) la información documentada que la organización considera necesaria para la eficacia del SGSI.

NOTA. El grado de información documentada para un SGSI puede variar de una organización a otra debido a:

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

2) la complejidad de los procesos y sus interacciones;

3) la competencia de las personas.

7.5.2 Creación y actualización

Al crear y actualizar información documentada, la organización debe asegurar que lo siguiente sea apropiado:

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

b) el formato (por ejemplo; lenguaje, versión del software, gráficos) y el medio (por ejemplo; papel, electrónico);

c) la revisión y la aprobación respecto de su pertinencia y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el SGSI y por esta norma se debe controlar para asegurar que:

a) esté disponible y apta para su uso, cuándo y dónde sea necesario;

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

Para controlar la información documentada, la organización debe tratar las actividades siguientes, cuando corresponda:

c) la distribución, el acceso, la recuperación y el uso;

d) el almacenamiento y la preservación, incluyendo la preservación de la legibilidad;

e) el control de cambios (por ejemplo, el control de versiones);

f) la conservación y la disposición final.

Se debe identificar de modo apropiado y controlar la información documentada de origen externo, que la organización considera necesaria para la planificación y la operación del SGSI.

NOTA Acceso implica tomar una decisión en relación al permiso de sólo lectura o el permiso y la autoridad de lectura y modificación de la información documentada, etc.

8 OPERACIÓN

8.1 Planificación y control operativo

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 6.1. La organización también debe implementar los planes para lograr los objetivos de seguridad de la información determinados en 6.2.

La organización debe conservar información documentada en el grado necesario para tener confianza en que los procesos se han realizado según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de cambios no intencionales, tomando las acciones necesarias para mitigar cualquier efecto adverso, cuando corresponda.

La organización debe asegurar que se determinan y controlan los procesos provistos por terceras partes.

8.2 Evaluación del riesgo a la seguridad de la información

La organización debe realizar evaluaciones del riesgo a la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en 6.1.2.a).

La organización debe conservar información documentada sobre los resultados de las evaluaciones del riesgo a la seguridad de la información.

8.3 Tratamiento del riesgo a la seguridad de la información

La organización debe implementar el plan de tratamiento del riesgo a la seguridad de la información.

La organización debe conservar información documentada sobre los resultados del tratamiento del riesgo a la seguridad de la información.

9 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

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

La organización debe determinar:

a) qué se necesita seguir y medir, incluyendo los procesos y los controles de seguridad de la información;

b) los métodos para realizar seguimiento, medición, análisis y evaluación, cuando corresponda, para asegurar resultados válidos;

NOTA. Para considerarlos válidos se recomienda que los métodos seleccionados produzcan resultados comparables y reproducibles.

c) cuándo se debe realizar seguimiento y medición;

d) quién debe realizar seguimiento y medición;

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

f) quién debe analizar y evaluar estos resultados.

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

9.2 Auditoría interna

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información acerca de si el SGSI:

a) es conforme con

1) los requisitos de la propia organización para su SGSI;

2) los requisitos de esta norma;

b) se implementa y mantiene eficazmente.

La organización debe:

c) planificar, establecer, implementar y mantener uno o más programas de auditoría, incluyendo la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la presentación de informes. El o los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas;

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

e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;

f) asegurar que los resultados de las auditorías se informen a la dirección pertinente;

g) conservar información documentada como evidencia del o los programas y los resultados de auditoría.

9.3 Revisión por parte de la dirección

La alta dirección debe revisar el SGSI de la organización a intervalos planificados para asegurar que continúa siendo pertinente, adecuado y eficaz.

La revisión por parte de la dirección debe incluir consideraciones acerca de:

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

b) los cambios en cuestiones internas y externas que sean pertinentes al SGSI;

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

   1) no conformidades y acciones correctivas;

   2) resultados del seguimiento y las mediciones;

   3) resultados de auditoría;

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

d) la retroalimentación de las partes interesadas;

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

f) las oportunidades de mejora continua.

Las salidas de la revisión por parte de la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios al SGSI.

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

10 MEJORA

10.1 No conformidad y acción correctiva

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar ante la no conformidad y, cuando corresponda:

   1) realizar acciones para controlarla y corregirla;

   2) actuar sobre las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, de manera de evitar que ésta se repita u ocurra en alguna otra parte, mediante:

   1) la revisión de la no conformidad;

   2) la determinación de las causas de la no conformidad;

   3) la determinación de la existencia de no conformidades similares, o su potencial existencia;

c) implementar todas las acciones necesarias;

d) revisar la eficacia de todas las acciones correctivas realizadas;

e) realizar los cambios al SGSI, de ser necesario.

Las acciones correctivas deben ser apropiadas 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 todas las acciones realizadas posteriormente;

g) los resultados de todas las acciones correctivas.

10.2 Mejora continua

La organización debe mejorar continuamente la pertinencia, la adecuación y la eficacia del SGSI.

Anexo A
(Normativo)

Objetivos de control y controles de referencia

Los objetivos de control y los controles indicados en la tabla A.1 se obtienen de manera directa y están alineados con aquellos indicados en los capítulos 5 a 18 de la ISO/IEC 27002:2013 y se deben utilizar 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	**Orientación de la dirección para la seguridad de la información**	
Objetivo: Proporcionar la orientación y el apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y las leyes y regulaciones pertinentes.		
A.5.1.1	Políticas de seguridad de la información	*Control* Se debe: – definir un conjunto de políticas para la seguridad de la información, – aprobarlas por la dirección, y – publicarlas y comunicarlas a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas de seguridad de la información	*Control* Las políticas de seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar que continúan siendo apropiadas, adecuadas y eficaces.
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 la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades relativas a la seguridad de la información.
A.6.1.2	Segregación de funciones	*Control* Se deben segregar las obligaciones y las áreas de responsabilidad incompatibles para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener los contactos apropiados con grupos de interés especial u otras asociaciones profesionales y foros de especialistas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* En la gestión de proyectos, se debe considerar la seguridad de la información, independientemente del tipo de proyecto.

(continúa)

Tabla A.1 (continuación)

A.6.2	**Dispositivos móviles y 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 las medidas de seguridad adecuadas para gestionar los riesgos ocasionados por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se debe implementar una política y las medidas de seguridad adecuadas para proteger la información que se accede, procesa y almacena en las instalaciones de teletrabajo.
A.7	**Seguridad de los recursos humanos**	
A.7.1	**Antes del empleo**	
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean idóneos para los roles para los cuales se los considera.		
A.7.1.1	Investigación de antecedentes	*Control* Se debe realizar la verificación de antecedentes de todos los candidatos para el empleo de acuerdo con las leyes, regulaciones y reglas éticas pertinentes. Dicha verificación debe ser proporcional a los requisitos del negocio, a la clasificación de la información a ser accedida y a los riesgos percibidos.
A.7.1.2	Términos y condiciones de empleo	*Control* Los contratos laborales con empleados y contratistas deben establecer sus responsabilidades y las de la organización para con la seguridad de la información.
A.7.2	**Durante el empleo**	
Objetivo: Asegurar que los empleados y contratistas sean conscientes de sus responsabilidades con respecto a la seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe requerir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y los procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando sea pertinente los contratistas, deben recibir una concientización, educación y capacitación apropiadas, y actualizaciones regulares sobre las políticas y procedimientos organizacionales, que sean pertinentes a su tarea.
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal y comunicado para sancionar a los empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Desvinculación o cambio de puesto**	
Objetivo: Proteger los intereses de la organización como parte del proceso de desvinculación o cambio de puesto.		
A.7.3.1	Responsabilidades en la desvinculación o cambio de puesto	*Control* Se deben definir, comunicar y hacer cumplir, al empleado o contratista, las responsabilidades y las obligaciones relativas a la seguridad de la información que continúan vigentes luego de la desvinculación o cambio de puesto.

(continúa)

Tabla A.1 (continuación)

A.8	**Gestión de activos**	
A.8.1	**Responsabilidad por los activos**	
Objetivo: Identificar los activos de la organización y definir las responsabilidades apropiadas para su protección.		
A.8.1.1	Inventario de los activos	*Control* Se deben identificar los activos asociados a la información y a las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos contenidos en el inventario deben tener propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados a la información y a las instalaciones de procesamiento de la información.
A.8.1.4	Retorno de activos	*Control* Todos los usuarios, tanto empleados como de terceras partes, deben devolver todos los activos de la organización en su poder tras la terminación de su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	
Objetivo: Asegurar que la información reciba un nivel de protección apropiado de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en términos de los requisitos legales, su valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas.
A.8.2.2	Rotulado de la información	*Control* Se debe desarrollar e implementar un conjunto apropiado de procedimientos para rotular la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manipulación de los activos	*Control* Se deben desarrollar e implementar procedimientos para manipular la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.
A.8.3	**Manipulación de los medios**	
Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizadas de información almacenada en medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación de la información adoptado por la organización.
A.8.3.2	Disposición final de medios	*Control* Cuando los medios dejen de ser requeridos, se deben eliminar de forma segura, utilizando procedimientos formales.
A.8.3.3	Traslado de medios físicos	*Control* Los medios que contengan información se deben proteger contra accesos no autorizados, mal uso o corrupción durante el transporte.
A.9	**Control de accesos**	
A.9.1	**Requisitos del negocio para el control de accesos**	
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.		

(continúa)

Tabla A.1 (continuación)

A.9.1.1	Política de control de accesos	*Control* Se debe establecer, documentar y revisar una política de control de accesos basada en los requisitos del negocio y de la seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	*Control* Se debe proveer a los usuarios sólo el acceso a la red y a los servicios a los cuales han sido específicamente autorizados a utilizar.
A.9.2	**Gestión de accesos del usuario**	
Objetivo: Asegurar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Alta y baja de registros de usuario	*Control* Se debe implementar un proceso formal de alta y baja de registros del usuario para permitir la asignación de derechos de acceso.
A.9.2.2	Asignación de accesos del usuario	*Control* Se debe implementar un proceso formal para otorgar o revocar los derechos de acceso de todos los tipos de usuario a todos los sistemas y servicios.
A.9.2.3	Gestión de los derechos de acceso privilegiado	*Control* Se deben restringir y controlar la asignación y uso de los derechos de acceso privilegiado.
A.9.2.4	Gestión de la información secreta para la autenticación del usuario	*Control* Se debe controlar la asignación de información secreta de autenticación a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso del usuario	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
A.9.2.6	Remoción o ajuste de los derechos de acceso	*Control* Se deben eliminar tras la finalización de su empleo, contrato o acuerdo, o se deben ajustar a cualquier cambio, los derechos de acceso a la información y a las instalaciones de procesamiento de la información de todos los usuarios, tanto empleados como de terceras partes.
A.9.3	**Responsabilidades del usuario**	
Objetivo: Hacer a los usuarios responsables de custodiar su información para la autenticación.		
A.9.3.1	Uso de la información secreta para la autenticación	*Control* Se debe solicitar a los usuarios que sigan las prácticas de la organización referidas al uso de la información secreta para la autenticación.
A.9.4	**Control de acceso a los sistemas y a las aplicaciones**	
Objetivo: Prevenir el acceso no autorizado a los sistemas y las aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones de los sistemas de aplicaciones de acuerdo con la política de control de acceso.
A.9.4.2	Procedimientos seguros de inicio de sesión	*Control* Se debe controlar el acceso a los sistemas y a las aplicaciones mediante un procedimiento seguro de inicio de sesión, cuando lo requiera la política de control de acceso.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

(continúa)

Tabla A.1 (continuación)

A.9.4.4	Uso de herramientas con privilegios	*Control* Se debe restringir y controlar rigurosamente el uso de herramientas que podrían ser capaces de pasar por alto los controles del sistema o de las aplicaciones.
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: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política de uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas a lo largo de todo su ciclo de vida.
A.11 Protección física y del entorno		
A.11.1 Áreas seguras		
Objetivo: Impedir accesos físicos no autorizados, daños e interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad para proteger áreas que contengan información e instalaciones de procesamiento de información sensibles o críticas.
A.11.1.2	Controles de ingreso físico	*Control* Se deben proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se permita el acceso al personal autorizado.
A.11.1.3	Aseguramiento de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar la seguridad física a las oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y del entorno	*Control* Se debe diseñar y aplicar la protección física contra desastres naturales, ataques intencionales o accidentes.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para el trabajo en áreas seguras.
A.11.1.6	Áreas de carga y descarga	*Control* Se deben controlar los puntos de acceso, tales como las áreas de carga y descarga y otros puntos donde personas no autorizadas pueden llegar a entrar a las instalaciones y, de ser posible, se deben aislar de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2 Equipamiento		
Objetivo: Impedir la pérdida, el daño, el robo o el compromiso de los activos así como la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	*Control* Se debe ubicar y proteger el equipamiento de manera tal que se reduzcan los riesgos ocasionados por amenazas y peligros del entorno, y las oportunidades de acceso no autorizado.

(continúa)

Tabla A.1 (continuación)

A.11.2.2	Elementos de soporte	*Control* Se debe proteger al equipamiento de fallas en el suministro eléctrico o de otras interrupciones ocasionadas por fallas en elementos de soporte.
A.11.2.3	Seguridad del cableado	*Control* El cableado de suministro eléctrico y de telecomunicaciones que transporta datos o que da soporte a servicios de información se debe proteger de intercepciones, interferencias o daños.
A.11.2.4	Mantenimiento del equipamiento	*Control* El equipamiento debe recibir un mantenimiento correcto para asegurar su continua disponibilidad e integridad.
A.11.2.5	Retiro de activos	*Control* No se deben retirar del sitio: equipamiento, información o software sin previa autorización.
A.11.2.6	Seguridad del equipamiento y los activos fuera de la organización	*Control* Se debe aplicar seguridad a los activos fuera de la organización teniendo en cuenta los diferentes riesgos de trabajar fuera de sus instalaciones.
A.11.2.7	Disposición final segura o reutilización del equipamiento	*Control* Se deben verificar todos los componentes del equipamiento que contengan medios de almacenamiento para asegurar que, antes de su disposición final o reutilización, se haya eliminado o sobrescrito de manera segura, cualquier dato sensible y software licenciado.
A.11.2.8	Equipamiento desatendido de usuario	*Control* Los usuarios deben asegurar que el equipamiento desatendido tenga la protección apropiada.
A.11.2.9	Política de escritorio y de pantalla limpios	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.
A.12	**Seguridad de las operaciones**	
A.12.1	**Procedimientos y responsabilidades operativos**	
Objetivo: Garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.		
A.12.1.1	Procedimientos operativos documentados	*Control* Se deben documentar los procedimientos operativos y deben estar disponibles para todos los usuarios que los necesiten.
A.12.1.2	Gestión del cambio	*Control* Se deben controlar los cambios en la organización, los procesos de negocio, las instalaciones de procesamiento de información y los sistemas que afecten a la seguridad de la información.
A.12.1.3	Gestión de la capacidad	*Control* Se debe realizar seguimiento y ajustar el uso de recursos y se deben realizar las proyecciones de futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y producción	*Control* Se deben separar los entornos de desarrollo, pruebas y producción para reducir los riesgos de accesos no autorizados o cambios en el entorno de producción.

(continúa)

Tabla A.1 (continuación)

A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso.		
A.12.2.1	Controles contra código malicioso	*Control* Se deben implementar los controles de detección, prevención y recuperación para la protección contra software malicioso, combinados con la concientización apropiada de los usuarios.
A.12.3 Resguardo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Resguardo de la información	*Control* Se deben hacer copias para el resguardo de la información, el software y los sistemas, y se las debe someter a pruebas periódicamente de acuerdo con la política acordada de resguardo.
A.12.4 Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	*Control* Se deben producir, conservar y revisar periódicamente los registros de eventos en los cuales se registren las actividades de los usuarios, las excepciones, los errores y los eventos de seguridad de la información.
A.12.4.2	Protección de la información de los registros	*Control* Las instalaciones de procesamiento de los registros y la información de registros se deben proteger contra manipulación y accesos no autorizados.
A.12.4.3	Registros de administradores y operadores	*Control* Se debe llevar registro de las actividades de los administradores y operadores del sistema, y se deben proteger y revisar periódicamente los registros.
A.12.4.4	Sincronización de los relojes	*Control* Dentro de una organización o dominio de seguridad, se deben sincronizar los relojes de todos los sistemas pertinentes de procesamiento de información de acuerdo a una única fuente de tiempo de referencia.
A.12.5 Control del software de producción		
Objetivo: Asegurar la integridad de los sistemas de producción.		
A.12.5.1	Instalación del software en los sistemas de producción	*Control* Se deben implementar procedimientos para controlar la instalación de software en los sistemas de producción.
A.12.6 Gestión de las vulnerabilidades técnicas		
Objetivo: Prevenir la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Control de las vulnerabilidades técnicas	*Control* Se debe obtener, de manera oportuna, información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas para tratar los riesgos asociados.
A.12.6.2	Restricciones a la instalación de software	*Control* Se deben establecer e implementar reglas que gobiernen la instalación de software por parte de los usuarios.

(continúa)

Tabla A.1 (continuación)

A.12.7 Consideraciones para las auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas de producción.		
A.12.7.1	Controles de la auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que involucren la verificación de los sistemas de producción se deben planificar cuidadosamente y acordar a fin de minimizar las interrupciones de los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de la red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información que la soportan.		
A.13.1.1	Controles de red	*Control* Se deben gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar e incluir en cualquier acuerdo de servicios de red los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sean servicios provistos por la organización o terceras partes.
A.13.1.3	Segregación en redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información, se deben segregar en más de una red.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de información a través del uso de todo tipo de instalación de comunicaciones.
A.13.2.2	Acuerdos de transferencia de información	*Control* Los acuerdos deben abordar la transferencia segura de la información de negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger apropiadamente la información involucrada en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad	*Control* Se deben identificar, revisar periódicamente y documentar los requisitos para que los acuerdos de confidencialidad reflejen las necesidades de la organización respecto a la protección de su información.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proveen servicios a través de redes públicas.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	*Control* Se deben incluir los requisitos relacionados con la seguridad de la información dentro de los requisitos para los nuevos sistemas de información o las mejoras de los existentes.

(continúa)

Tabla A.1 (continuación)

A.14.1.2	Aseguramiento de los servicios de aplicaciones sobre redes públicas	*Control* La información involucrada en servicios de aplicaciones que atraviesa redes públicas se debe proteger contra actividades fraudulentas, litigios contractuales y divulgaciones y modificaciones no autorizadas.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	*Control* Se debe proteger la información involucrada en las transacciones de los servicios de aplicaciones para prevenir transmisiones incompletas, *ruteo* erróneo, alteración no autorizada de los mensajes, divulgación no autorizada, duplicación o repetición no autorizadas de los mensajes.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida del desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer reglas para el desarrollo de software y de sistemas y se las debe aplicar a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en los sistemas	*Control* Se deben controlar los cambios a los sistemas dentro del ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisiones técnicas de las aplicaciones luego de cambios en la plataforma de producción	*Control* Cuando se cambian los sistemas de producción, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no se produzca un impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones a los cambios en los paquetes de software	*Control* Se deben desalentar las modificaciones en los paquetes de software, limitarlas a los cambios necesarios y controlar estrictamente todos los cambios.
A.14.2.5	Principios de seguridad en el desarrollo de sistemas	*Control* Se deben establecer, documentar, mantener y aplicar los principios de seguridad para el desarrollo de sistemas seguros, en la implementación de sistemas de información.
A.14.2.6	Entorno seguro de desarrollo	*Control* Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo para que los esfuerzos de desarrollo e integración cubran todo el ciclo de vida de desarrollo de los sistemas.
A.14.2.7	Desarrollo provisto por terceras partes	*Control* La organización debe supervisar y realizar el seguimiento de las actividades de desarrollo de los sistemas provistas por terceras partes.
A.14.2.8	Pruebas de seguridad de los sistemas	*Control* Se deben realizar pruebas de las funcionalidades de seguridad durante el desarrollo.
A.14.2.9	Pruebas de aceptación de los sistemas	*Control* Se deben establecer criterios y programas de pruebas de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas.

(continúa)

Tabla A.1 (continuación)

A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos utilizados para las pruebas.		
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar cuidadosamente, proteger y controlar.
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar la protección de los activos de la organización a los cuales tienen acceso los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	*Control* Se deben acordar con el proveedor y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.
A.15.1.2	Tratamiento de la seguridad en los acuerdos con los proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de las tecnologías de la información y las comunicaciones	*Control* Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos a la seguridad de la información asociados a la cadena de suministro de servicios y productos de las tecnologías de la información y las comunicaciones.
A.15.2 Gestión de la entrega de servicios prestados por los proveedores		
Objetivo: Mantener un nivel acordado de seguridad de la información y de prestación de servicio alineados con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios prestados por los proveedores	*Control* Las organizaciones deben seguir, revisar y auditar periódicamente la entrega de los servicios prestados por proveedores.
A.15.2.2	Gestión de cambios en los servicios prestados por proveedores	*Control* Los cambios en la prestación de los servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se deben gestionar, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados y la reevaluación de los riesgos.
A.16 Gestión de los incidentes de seguridad de la información		
A.16.1 Gestión de los incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y las vulnerabilidades de la seguridad.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Presentación de informes sobre los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de canales de gestión apropiados, tan pronto como sea posible.

(continúa)

Tabla A.1 (continuación)

A.16.1.3	Presentación de informes sobre las vulnerabilidades de seguridad de la información	*Control* Se debe requerir que los empleados y contratistas que utilicen los sistemas y servicios de información de la organización informen cualquier vulnerabilidad de seguridad de la información observada o sospechada en sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	*Control* Se deben evaluar los eventos de seguridad de la información y decidir si se los debe clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a los incidentes de seguridad de la información	*Control* Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje a partir de los incidentes de seguridad de la información	*Control* Se debe utilizar el conocimiento obtenido del análisis y resolución de los incidentes de seguridad de la información para reducir la probabilidad o el impacto de futuros incidentes.
A.16.1.7	Recolección de la evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que se pueda utilizar como evidencia.
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de la continuidad del negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos de seguridad de la información y de la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o un desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y valoración de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de la continuidad de la seguridad de la información, establecidos e implementados, para asegurar que sean válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	*Control* Las instalaciones de procesamiento de la información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad.

(continúa)

Tabla A.1 (fin)

A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar la violación de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación y de los requisitos contractuales aplicables	*Control* Todos los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir con estos requisitos, se deben identificar explícitamente, documentar y mantener actualizados para cada sistema de información, y para la organización.
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietarios.
A.18.1.3	Protección de los registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado o divulgación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de la información personal	*Control* Se debe asegurar la privacidad y la protección de la información personal, según lo requiera la legislación y regulación pertinente, cuando corresponda.
A.18.1.5	Regulación de controles criptográficos	*Control* Los controles criptográficos se deben utilizar cumpliendo todos los acuerdos, leyes y regulaciones pertinentes.
A.18.2 Revisión de la seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere 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 la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar en forma independiente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento de las políticas y las normas de seguridad	*Control* El nivel gerencial debe revisar periódicamente que el cumplimiento de los procesos y procedimientos de información en su área de responsabilidad, se alinee con las políticas, las normas y cualquier otro requisito de seguridad apropiados.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para verificar que cumplan con las políticas y las normas de seguridad de la información de la organización.

Bibliografía ISO

[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*

Anexo B - IRAM
(Informativo)

Bibliografía

En la revisión de esta norma se han tenido en cuenta los antecedentes siguientes:

IRAM - INSTITUTO ARGENTINO DE NORMALIZACIÓN
IRAM-ISO/IEC 27001:2007 - Tecnología de la información. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
ISO/IEC 27001:2013 - Information technology. Security techniques. Information security management systems. Requirements.

Anexo C - IRAM
(Informativo)

Integrantes de los organismos de estudio

La revisión de esta norma ha estado a cargo de los organismos respectivos, integrados en la forma siguiente:

Subcomité de Seguridad en tecnología de la información

Integrante		Representa a:
Ing.	Jorge ETEROVIC	UNIVERSIDAD NACIONAL DE LA MATANZA
Lic.	Graciela FRIGERI	UNIVERSIDAD CATÓLICA DE SALTA (UCASAL)
Ing.	Gustavo GARFINKIEL	MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL
Ing.	Fernando LA ROSA	TRADITUM S.A./HL7 ARGENTINA
Mg.	Marcia MAGGIORE	UNIVERSIDAD DE BUENOS AIRES - FACULTAD DE CIENCIAS ECONÓMICAS (UBA-FCE)
Ing.	Marcela MEYORÍN	UNIVERSIDAD MARINA MERCANTE
Sr.	César MORENO	GRIENSU S.A.
Lic.	Fernando RADICCHI	BANCO DE LA NACIÓN ARGENTINA
Mg.	Susana ROMANIZ	FACULTAD REGIONAL SANTA FE (UTN)
Ing.	Pablo ROMANOS	UNIVERSIDAD DE LA MARINA MERCANTE
Dr.	Raúl SAROKA	UNIVERSIDAD DE BUENOS AIRES - FACULTAD DE CIENCIAS ECONÓMICAS (UBA-FCE)
Ing.	Javier SOLA	IATREION SOFTWARE
Ing.	Jorge CEBALLOS	IRAM
Ing.	Julieta JALIL QUIROGA	IRAM
Ing.	Adriana NUÑEZ	IRAM
Lic.	Verónica MARINELLI	IRAM

Comité General de Normas (C.G.N.)

Integrante		Integrante	
Ing.	Alberto BUSTOS ROYER	Dr.	Ricardo MACCHI
Dr.	José M. CARACUEL	Ing.	Jorge MANGOSIO
Lic.	Alberto CERINI	Téc.	Hugo D. MARCH
Ing.	Ramiro FERNÁNDEZ	Lic.	Héctor MUGICA
Lic.	Alicia GUTIÉRREZ	Ing.	Tulio PALACIOS
Ing.	Jorge KOSTIC	Ing.	Raúl DELLA PORTA