NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27001
2014

Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI
Calle de La Prosa 104, San Borja (Lima 41) Apartado 145 Lima, Perú

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

INFORMATION TECHNOLOGY. Security techniques. Information security management systems — Requirements

(EQV. ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR 1 Information technology -- Security techniques -- Information security management systems – Requirements)

2014-11-20
2ª Edición

R.0129-2014/CNB-INDECOPI. Publicada el 2014-12-01 Precio basado en 36 páginas
I.C.S.: 35.040 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología, información, técnicas, seguridad, sistema de gestión, requisitos

INDECOPI

Calle de La Prosa 104, San Borja
Lima- Perú
Tel.: +51 1 224-7777
Fax.: +51 1 224-1715
sacreclamo@indecopi.gob.pe
www.indecopi.gob.pe

ÍNDICE

PREFACIO

A. RESEÑA HISTÓRICA

A.1 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a junio del 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems – Requirements y la ISO/IEC 27001:2013/COR 1 2013 Information Technology – Security techniques – Information security management systems – Requirements

A.2 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias -CNB-, con fecha 2014-08-19, el PNTP-ISO/IEC 27001:2014, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2014-10-18. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos,** 2ª Edición, el 01 de diciembre de 2014.

A.3 Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1 . La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia a las Guías Peruanas GP 001:1995 y GP 002:1995.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	GS1 PERU
Presidente	Roberto Puyó
Secretaria	Mary Wong

ENTIDAD	REPRESENTANTE
B2IMPROVE S.A.C.	Belén Alvarado
CONSULTOR	Carlos Horna
DELOITTE & TOUCHE S.R.L.	Diana Lagos
DMS Perú S.A.C.	Adela Bárcenas Walter Equizabal
INDECOPI	Ivan Ancco
NSF INASSA SAC.	Raúl Miranda
SUPERINTENDENCIA DE ADMINISTRACION TRIBUTARIA – SUNAT	Daniel Llanos
GS1 PERU	Sara Carrión
CONTRALORÍA GENERAL DE LA REPÚBLICA	Marco Bermúdez Joel Mercado
FOLIUM S.A.C.	Roberto Huby
ONGEI	Ricardo Dioses
Facultad de Ciencias e Ingeniería - PUCP	Viktor Khlebnikov Willy Carrera
ITICSEC S.A.C.	Maurice Frayssinet
Consultora	Judith Blanco Jallurana

PRÓLOGO
(ISO)

ISO (la Organización Internacional para la Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los órganos nacionales que son miembros de ISO o de IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para ocuparse de campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en enlace con ISO y con IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Se redactan las Normas Internacionales en concordancia con las reglas proporcionadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar las normas internacionales adoptadas por el comité técnico conjunto, se circulan a los órganos nacionales para su votación. La publicación como una Norma Internacional requiere la aprobación de al menos 75 % de los órganos nacionales que emiten un voto.

Se señala la posibilidad de que alguno de los elementos de este documento pueda estar sujeto a derechos de patentes. No se hará responsable a ISO e IEC de identificar cualquiera o todos los mencionados derechos de patentes.

ISO/IEC 27001 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1, Tecnología de la información, Sub-comité SC 27, Técnicas de seguridad de la TI.

Esta segunda edición cancela y reemplaza la primera edición (NTP-ISO/IEC 27001:2008), la cual se ha revisado técnicamente.

0. INTRODUCCIÓN (ISO)

0.1 Generalidades

Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente 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 de la organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca a escala en concordancia con las necesidades de la organización.

Las partes internas y externas pueden utilizar esta Norma Técnica peruana para evaluar la capacidad que tiene la organización de cumplir los requisitos de seguridad de la información de la propia organización.

El orden en el que se presentan los requisitos en esta Norma Técnica Peruana no refleja su importancia ni implica el orden en el que deben implementarse. Los elementos de la lista se enumeran únicamente para propósitos de referencia.

ISO/IEC 27000 describe una visión general y el vocabulario de los sistemas de seguridad de la información, haciendo referencia a la familia de normas del sistema de gestión de seguridad de la información (incluyendo ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4], con términos y definiciones relacionadas.

0.2 Compatibilidad con otras normas de sistemas de gestión

Esta Norma Técnica Peruana aplica la estructura de alto nivel, títulos de sub-clausulas idénticos, texto idéntico, términos comunes, y definiciones básicas proporcionadas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO Consolidado y, por lo tanto, mantiene 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 elijan operar un sistema de gestión único que satisfaga los requisitos de dos o más normas de sistemas de gestión.

---oooOooo---

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos

1. OBJETO Y CAMPO DE APLICACIÓN

Esta Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Excluir cualquiera de los requisitos especificados en las Cláusulas 4 a 10 no es aceptable cuando una organización declara conformidad con esta Norma Técnica Peruana.

2. REFERENCIAS NORMATIVAS

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

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

3. TÉRMINOS Y DEFINICIONES

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

4. CONTEXTO DE LA ORGANIZACION

4.1 Comprender la organización y su contexto

La organización debe determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este sistema de gestión de seguridad de la información.

NOTA: Determinar si estos aspectos se refiere a establecer el contexto externo e interno de la organización considerado en la Cláusula 5.3 de ISO 31000:2009[5].

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas relevantes al sistema de gestión de seguridad de la información; y

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

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

4.3 Determinar el 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) los aspectos externos e internos referidos en 4.1;

b) los requisitos referidos en 4.2; y

c) las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas 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 continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma Técnica Peruana.

5. LIDERAZGO

5.1 Liderazgo y compromiso

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

a) asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y 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 efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información;

e) asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s);

f) dirigiendo y apoyando a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información;

g) promoviendo la mejora continua; y

h) apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

5.2 Política

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

a) es apropiada al propósito de la organización;

b) incluye objetivos de seguridad de la información (véase 6.2) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información;

c) incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e

d) incluye un 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) estar comunicada dentro de la organización; y

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

5.3 Roles, responsabilidades y autoridades organizacionales

La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

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

a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana; y

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

NOTA: La alta dirección también puede asignar responsabilidades y la autoridad para reportar desempeño del sistema de gestión de seguridad de la información dentro de la organización.

6. PLANIFICACIÓN

6.1 Acciones para tratar los riesgos y las oportunidades

6.1.1 Generalidades

Cuando se planifica para el sistema de gestión de seguridad de la información, la organización debe considerar los asuntos referidos en el numeral 4.1 y los requisitos referidos en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para:

a) asegurar que el sistema de gestión de seguridad de la información pueda lograr su(s) resultado(s) esperado(s);

b) prevenir, o reducir, efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) acciones que traten estos riesgos y oportunidades; y

e) como

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

2) evaluar la efectividad de estas acciones.

6.1.2 Valoración del riesgo de seguridad de la información

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

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

1) los criterios de aceptación de los riesgos; y

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

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

c) identifique los riesgos de seguridad de la información

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

2) identificando a los propietarios de riesgos;

d) analice los riesgos de seguridad de la información:

1) valorando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse;

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

3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a); y

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

La organización debe retener información documentada sobre el proceso de valoración de riesgos de seguridad de la información.

6.1.3 Tratamiento de riesgos de seguridad de la información.

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

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

b) determinar todos los controles que son 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 se requiera, o identificarlos de cualquier fuente.

c) Comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario;

NOTA 1: El Anexo A contiene una lista integral de objetivos de control y controles. Los usuarios de esta Norma Técnica Peruana pueden dirigirse al Anexo A para asegurar que no se deje de lado ningún control necesario.

NOTA 2: Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles listados 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 (véase 6.1.3 b) y c)) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A;

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

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

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

NOTA: El proceso de valoración y tratamiento de riesgos de seguridad de la información en esta Norma Técnica Peruana se alinea con los principios y lineamientos genéricos proporcionados en ISO 31000[5]

6.2 Objetivos de seguridad de la información y planificación para conseguirlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

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

b) ser medibles (si es práctico);

c) tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos;

d) ser comunicados; y

e) ser actualizados según sea apropiado.

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

Cuando planifique cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

f) qué se hará;

g) qué recursos serán requeridos;

h) quién será responsable;

i) cuándo se culminará;

j) cómo los resultados serán evaluados.

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 la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información;

b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados;

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

d) Retener información documentada apropiada como evidencia de competencia.

NOTA: Las acciones aplicables pueden incluir, por ejemplo: la provisión de capacitación a, mentoría a, o reasignación de los actuales empleados; o la contratación de personas competentes.

7.3 Concientización

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

a) la política de seguridad de información;

b) su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y

c) las implicancias de no tener conformidad 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 relevantes al sistema de gestión de seguridad de la información incluyendo:

a) qué comunicar;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar; y

e) los procesos por los cuales la comunicación debe ser efectuada.

7.5 Información documentada

7.5.1 Generalidades

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

a) información documentada requerida por esta Norma Técnica Peruana; e

b) información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.

NOTA: La extensión de la información documentada para un sistema de gestión de seguridad de la información puede diferir 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; y

3) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza información documentada, la organización debe asegurar:

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

b) formato (por ejemplo el lenguaje, versión de software, gráficos) y medios (por ejemplo papel, electrónico) apropiados; y

c) revisión y aprobación apropiadas para su conveniencia y adecuación.

7.5.3 Información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por esta Norma Técnica Peruana se debe controlar para asegurar:

a) que esté disponible y sea conveniente para su uso donde y cuando sea necesaria; y

b) que esté protegida adecuadamente (por ejemplo de pérdida de confidencialidad, uso impropio, o pérdida de integridad).

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

c) distribución, acceso, recuperación y uso;

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

e) control de cambios (por ejemplo control de versiones); y

f) retención y disposición.

La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, debe ser identificada según sea apropiado y controlarse.

NOTA: El acceso implica una decisión respecto de la autorización de solamente ver la información documentada, o el permiso y la autoridad de ver y cambiar la información documentada, etc.

8. OPERACIÓN

8.1 Planificación y control operacional

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

La organización debe mantener información documentada en la medida necesaria para estar segura de que los procesos se han llevado a cabo tal como fueron planificados.

La organización debe controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurar que los procesos tercerizados son determinados y controlados.

8.2 Evaluación de riesgos de seguridad de la información

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

La organización debe retener información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

8.3 Tratamiento de riesgos de seguridad de la información

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

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

9. EVALUACIÓN DEL DESEMPEÑO

9.1 Monitoreo, medición, análisis y evaluación

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

La organización debe determinar:

a) qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información;

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

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

c) cuándo el monitoreo y medición debe ser realizado;

d) quién debe monitorear y medir;

e) cuándo los resultados del monitoreo y medición deben ser analizados y evaluados; y

f) quién debe analizar y evaluar estos resultados.

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

9.2 Auditoría interna

La organización debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

a) está en conformidad con

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

2) los requisitos de esta Norma Técnica Peruana;

b) está efectivamente implementado y mantenido.

La organización debe:

c) planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación. Los programas de auditoría deben tomar en consideración la importancia de los procesos concernientes y los resultados de auditorías previas;

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

e) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría;

f) asegurar que los resultados de las auditorías se reporten a los gerentes relevantes; y

g) retener información documentada como evidencia del (de los) programa(s) de auditoría y los resultados de la auditoría.

9.3 Revisión por la gerencia

La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.

La revisión por la gerencia debe incluir consideraciones de:

a) el estado de las acciones con relación a las revisiones anteriores por parte de la gerencia;

b) cambios en asuntos externos e internos que son relevantes al sistema de gestión de seguridad de la información;

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

1) no conformidades y acciones correctivas;

2) resultados del monitoreo y medición;

3) resultados de auditoría; y

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

d) retroalimentación de partes interesadas;

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

f) oportunidades para la mejora continua.

Los productos de la revisión por la gerencia deben incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de seguridad de la información.

La organización debe retener información documentada como evidencia de los resultados de revisiones por parte de la gerencia.

10. MEJORAS

10.1 No conformidades y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

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

1) tomar acción para controlarla y corregirla; y

2) ocuparse de las consecuencias;

b) evaluar la necesidad de la acción para eliminar las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar de las siguientes maneras:

1) revisando la no conformidad;

2) determinando las causas de la no conformidad; y

3) determinando si existen no conformidades similares o si podrían ocurrir potencialmente;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada; y

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

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

La organización debe retener información documentada como evidencia de:

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

g) los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la conveniencia, adecuación y efectividad 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 listados en la Tabla A.1 son directamente derivados desde y alineados con los listados en ISO/IEC 27002:2013[1], Cláusulas 5 a 18 y se utilizan en el contexto con el Apartado 6.1.3.

TABLA A.1 – Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Dirección de la gerencia para la seguridad de la información		
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.		
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 gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	*Control* Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.
A.6.1.3	Contacto con autoridades	*Control* Contactos apropiados con autoridades relevantes deben ser mantenidos.

Tabla A.1 *(continuación)*

A.6.1.4	Contacto con grupos especiales de interés	*Control* Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.
A.6.2 Dispositivos móviles y teletrabajo		
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	*Control* Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.
A.7 Seguridad de los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.		
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidades de la gerencia	*Control* La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.

A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	*Control* Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.
A.7.2.3	Proceso disciplinario	*Control* Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.
A.7.3 Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	*Control* Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.
A.8 Gestión de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	*Control* Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben ser propios.

Tabla A.8 *(continuación)*

A.8.1.3	Uso aceptable de los activos	*Control* Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.
A.8.1.4	Retorno de activos	*Control* Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.

A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.

Tabla A.8 *(continuación)*

A.8.3.2	Disposición de medios	*Control* Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de la empresa para el control de acceso		
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.		
A.9.1.1	Política de control de acceso	*Control* Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y servicios de red	*Control* Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.
A.9.2 Gestión de acceso de usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuarios	*Control* Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.
A.9.2.2	Aprovisionamiento de acceso a usuario	*Control* Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control* La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.
A.9.2.4	Gestión de información de autentificación secreta de usuarios	*Control* La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.

Tabla A.9 *(continuación)*

A.9.2.5	Revisión de derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Remoción o ajuste de derechos de acceso	*Control* Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.
A.9.3 Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.		
A.9.3.1	Uso de información de autentificación secreta	*Control* Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.
A.9.4 Control de acceso a sistema y aplicación		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos de ingreso seguro	*Control* Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* El acceso al código fuente de los programas debe ser restringido.

A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.
A.10.1.2	Gestión de claves	*Control* Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.
A.11 Seguridad física y ambiental		
A.11.1 Áreas seguras		
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.
A.11.1.2	Controles de ingreso físico	*Control* Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	*Control* Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
A.11.1.5	Trabajo en áreas seguras	*Control* Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.

Tabla A.11 *(continuación)*

A.11.1.6	Áreas de despacho y carga	*Control* Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de los equipos	*Control* Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.
A.11.2.2	Servicios de suministro	*Control* Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.
A.11.2.5	Remoción de activos	*Control* Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.

Tabla A.11 *(continuación)*

A.11.2.7	Disposición o reutilización segura de equipos	*Control* Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	*Control* Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.

A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operativas		
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.		
A.12.1.1	Procedimientos operativos documentados	*Control* Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión del cambio	*Control* Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de la capacidad	*Control* El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	*Control* Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

Tabla A.12 *(continuación)*

A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	*Control* Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.
A.12.3 Respaldo		
Objetivo: Proteger contra la pérdida de datos		
A.12.3.1	Respaldo de la información	*Control* Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
A.12.4 Registros y monitoreo		
Objetivo: Registrar eventos y generar evidencia		
A.12.4.1	Registro de eventos	*Control* Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.
A.12.4.2	Protección de información de registros.	*Control* Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de reloj	*Control* Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.
A.12.5 Control del software operacional		
Objetivo: Asegurar la integridad de los sistemas operacionales		
A.12.5.1	Instalación de software en sistemas operacionales	*Control* Procedimientos deben ser implementados s para controlar la instalación de software en sistemas operacionales.

Tabla A.12 *(continuación)*

A.12.6 Gestión de vulnerabilidad técnica		
Objetivo: Prevenir la explotación de vulnerabilidades técnicas		
A.12.6.1	Gestión de vulnerabilidades técnicas	*Control* Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.
A.12.7 Consideraciones para la auditoría de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de seguridad de la red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.		
A.13.1.1	Controles de la red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.
A.13.1.2	Seguridad de servicios de red	*Control* Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.
A.13.1.3	Segregación en redes	*Control* Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		

Tabla A.13 *(continuación)*

A.13.2.1	Políticas y procedimientos de transferencia de la información	*Control* Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdo sobre transferencia de información	*Control* Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.
A.13.2.3	Mensajes electrónicos	*Control* La información involucrada en mensajería electrónica debe ser protegida apropiadamente.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.
A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	*Control* La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.
A.14.1.3	Protección de transacciones en servicios de aplicación	*Control* La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.

Tabla A.14 *(continuación)*

A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambio del sistema	*Control* Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	*Control* Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones sobre cambios a los paquetes de software	*Control* Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.
A.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.
A.14.2.8	Pruebas de seguridad del sistema	*Control* Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.

Tabla A.14 *(continuación)*

A.14.2.9	Pruebas de aceptación del sistema	*Control* Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de datos utilizados para las pruebas		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	*Control* Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	*Control* Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.
A.15.2 Gestión de entrega de servicios del proveedor		
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.		
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	*Control* Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.

Tabla A.15 *(continuación)*

A.15.2.2	Gestión de cambios a los servicios de proveedores	*Control* Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de 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 consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados 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 adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.

Tabla A.16 *(continuación)*

A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización		
A.17.1.1	Planificación de continuidad de seguridad de la información	*Control* La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.
A.17.1.2	Implementación de continuidad de 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 seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	*Control* La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información		
A.17.2.1	Instalaciones de procesamiento de la información	*Control* Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento con requisitos legales y contractuales		
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.		

Tabla A.18 *(continuación)*

A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	*Control* Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	*Control* Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.
A.18.1.3	Protección de registros	*Control* Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de datos personales.	*Control* La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.
A.18.1.5	Regulación de controles criptográficos	*Control* Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.

Tabla A.18 *(continuación)*

A.18.2.2	Cumplimiento de políticas y normas de seguridad	*Control* Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de 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 (Tecnología de la información – Técnicas de seguridad – Código de práctica para controles de seguridad de la información)*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance (Tecnología de la información – Técnicas de seguridad – Guía de implementación del sistema de gestión de seguridad de la información)*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement* (*Tecnología de la información – Técnicas de seguridad – Gestión de seguridad de la información – Medición)*

[4] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management* (*Tecnología de la información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información)*

[5] ISO 31000:2009, *Risk management — Principles and guidelines(Gestión de riesgos – Principios y lineamientos)*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement – Procedures specific to ISO*, 2012 *(Directivas, Parte 1, Suplemento Consolidado de ISO – Procedimientos específicos a ISO, 2012)*