

NORMA

ISO 27001:2013

**SISTEMA DE GESTIÓN
SEGURIDAD DE INFORMACIÓN SGSI**

WHEN YOU NEED TO BE SURE



Prohibida la reproducción por cualquier medio sin la autorización escrita por parte de la Dirección General.

Member of the SGS Group (Société Générale de Surveillance)

NORMA
INTERNACIONAL
ISO/IEC
27001

Segunda edición

2013-10-01

Tecnología de la Información -

Técnicas de Seguridad

Sistemas de Gestión

de la Seguridad de la Información - Requisitos

*Technologies de l'information — Techniques de sécurité — Systèmes
de management de la sécurité de l'information — Exigences*

Prólogo

ISO (Organización Internacional para la Estandarización) y el IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la estandarización a nivel internacional. Los entes nacionales que forman parte de ISO e IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos formados por la misma organización para ocuparse de campos específicos de la actividad técnica. Los comités técnicos de ISO y la IEC colaboran en campos de mutuo interés. Otras organizaciones y entidades gubernamentales y no gubernamentales, en coordinación con ISO y la IEC, también participan en esta labor. En el campo de la tecnología de la información, ISO y la IEC han establecido un comité técnico colectivo, ISO/IEC JTC 1.

Se ha seleccionado normas internacionales de acuerdo a las reglas dadas en las Directivas ISO /IEC, Parte 2.

El principal objetivo del comité técnico colectivo es elaborar las Normas Internacionales. Las Normas Internacionales diseñadas por el comité técnico colectivo son circuladas a los entes nacionales para ser sometidos a votación. La publicación de la Norma Internacional requiere de la aprobación de al menos el 75% de los entes nacionales con derecho a voto.

Se tiene un especial cuidado sobre la posibilidad de que uno de los elementos del presente documento sean sujetos a derechos de patente.

ISO y la IEC no se hacen responsables de la identificación de alguna o todas los derechos de patente.

ISO/IEC 27001 fue elaborado por el Comité Técnico Colectivo ISO/IEC JTC 1, *Tecnología de la Información*, el Sub-Comité SC27, IT, *Técnicas de Seguridad*.

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

0 Introducción

0.1 General

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

El sistema de seguridad de la información conserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y garantiza, a las partes interesadas, que los riesgos sean manejados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información forme parte y se integre con los procesos y estructuras de gestión integral de la organización y que se considere a la seguridad de la información en el diseño de los procesos, sistemas de la información y controles.

Se espera que la implementación del sistema de gestión de la seguridad de la información se amplíe de acuerdo a las necesidades de la organización.

Esta Norma Internacional puede ser utilizada por las partes internas y externas para la evaluación de la capacidad de la información para cumplir con sus propios requisitos de seguridad de la información. El orden en que son presentados los requisitos de la presente Norma Internacional no refleja su importancia ni implica un orden en el cual deben ser implementados. La lista de ítems son enumerados sólo de manera referencial.

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

0.2 Compatibilidad con otras normas del sistema de gestión

La presente Norma Internacional aplica la estructura de nivel alto, títulos de sub-capítulos idénticos, textos idénticos, términos comunes y definiciones básicas definidas en el Anexo SL del ISO/IEC Directivas, Parte 1, Consolidado del Suplemento ISO, y por lo tanto mantiene compatibilidad con otras normas del sistema de gestión que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL será de gran utilidad para las organizaciones que decidan operar con un único sistema de gestión que cumpla con los requisitos de dos o más normas del sistema de gestión

Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos

1 Alcance

Esta Norma Internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de seguridad de la información dentro del contexto de la organización. Esta Norma Internacional también incluye los requisitos para la evaluación y tratamiento de los riesgos de la información adaptados a las necesidades de la organización. Los requisitos establecidos en la Norma Internacional son genéricos y han sido elaborados para ser aplicados en todas las organizaciones, independientemente del tipo, tamaño o naturaleza. Excluyendo algunos de los requisitos especificados en las Cláusulas del 4 al 10, no se acepta que una organización asegure conformidad con la Norma Internacional.

2 Referencias Normativas

Los siguientes documentos, parte o en su totalidad, constituyen referencias normativas en el presente documento y son indispensables para su aplicación. Para las referencias que contienen fechas, aplica únicamente la edición citada. Para las referencias que no contienen fechas, aplica la última edición del documento en mención (incluyendo las enmiendas).

3 Términos y definiciones

Para el propósito del presente documento, aplica los términos y definiciones dados en ISO/IEC 27000.

4 Contexto de la Organización

4.1 Conocimiento de la organización y su contexto

La organización deberá determinar los asuntos internos y externos que sean relevantes para su propósito y que afectan su capacidad para lograr el o los resultados esperados de su sistema de gestión de la organización.

NOTA: Determinar estos asuntos implica establecer el contexto interno y externo de la organización considerados en la Cláusula 5.3 del ISO 31000:2009 [5].

4.2 Conocimiento de las necesidades y expectativas de las partes interesadas

La Organización deberá determinar:

- a) Las partes interesadas que sean relevantes para el sistema de gestión de la seguridad de la información; y

b) Los requisitos de estas partes interesadas con respecto a la seguridad de la información.

NOTA: Los requisitos de las partes interesadas deben incluir los requisitos legales y regulatorios y las obligaciones contractuales.

4.3 Determinación del alcance del sistema de seguridad de la información

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

Al determinar este alcance, la organización deberá considerar:

- a) Los asuntos internos y externos mencionados en 4.1;
- b) Los requisitos mencionados en el 4.2; y
- c) Las interfaces y dependencias entre las actividades desempeñadas por la organización, y aquellas que desarrollan otras organizaciones.

(E)

Establecida
Implementada
Mantinida

El alcance deberá estar disponible como información documentada. OK

4.4 Sistema de Gestión de la Seguridad de la Información

La organización deberá establecer, implementar, mantener y mejorar de manera continua el sistema de seguridad de la información, de acuerdo a los requisitos de la Norma Internacional

5 Liderazgo

5.1 Liderazgo y compromiso

La Alta Dirección deberá demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información mediante las siguientes acciones:

- a) Garantizando el establecimiento de la política y objetivos de la seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;
- b) Garantizando la integración de los requisitos del sistema de gestión de la información dentro de los procesos de la organización;
- c) Garantizando la disponibilidad de los recursos necesarios para el sistema de gestión de la seguridad de la información;
- d) Comunicando la importancia de una gestión efectiva de seguridad de la información y de adecuarse a los requisitos del sistema de gestión de la seguridad de la información;
- e) Garantizando que el sistema de seguridad de la información logre sus resultados esperados;
- f) Dirigiendo y dando soporte a las personas para que contribuyan con la efectividad del sistema de gestión de la seguridad de la información;
- g) Promoviendo la mejora continua; y

h) Apoyando las funciones de la gerencia que permitan demostrar su liderazgo siempre que corresponda a sus áreas de responsabilidad.

5.2 Política

OK ✓

La Alta Dirección deberá establecer una política de seguridad de la información que:

- ✓ a) Sea adecuada al propósito de la organización; (alineado con la misión)
- b) Incluya los objetivos de seguridad de la información (ver 6.2) o proporcione un esquema para la determinación de los objetivos de la seguridad de la información;
- c) Incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información; e
(integridad, disponibilidad, confidencialidad)
- ✓ d) Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información deberá:

- e) Estar disponible como información documentada;
- f) Ser comunicada dentro de la organización; y
- g) Estar disponible para las partes interesadas, de la manera que estimen adecuada.

5.3 Funciones, responsabilidades y autoridad de la organización

La Alta Gerencia deberá garantizar que se asigne y comunique las responsabilidades y autoridad para los roles relacionados con la seguridad de la información.

La Alta Dirección deberá asignar la responsabilidad y autoridad para:

- a) Garantizar que el sistema de gestión de seguridad de la información se adapte a los requisitos de esta Norma Internacional: e
- b) Informar acerca del desempeño del sistema de gestión de seguridad de la información a la Alta Gerencia.

NOTA: La Alta Gerencia también asignaría responsabilidades y autoridad para informar acerca del desempeño del sistema de gestión de seguridad de la información dentro de la organización.

6 Planificación

6.1 Acciones para enfrentar los riesgos y las oportunidades

6.1.1 General

Al planificar el sistema de gestión de la seguridad de la información, la organización deberá considerar los temas referidos al punto 4.1 y a los requisitos mencionados en el punto 4.2, y determinar los riesgos y oportunidades que deben orientarse a:

- a) Garantizar que el sistema de gestión de seguridad de la información logre los resultados esperados;
- b) Evitar o reducir efectos indeseados; y
- c) Lograr la mejora continua

La organización deberá planificar:

- d) Las acciones destinadas a manejar estos riesgos y oportunidades; y

e) Cómo

- 1) Integrar e implementar las acciones dentro de los procesos del sistema de gestión de seguridad de la información; y

- 2) Evaluar la efectividad de estas acciones

6.1.2 Evaluación de los riesgos de seguridad de la información

La organización deberá definir y aplicar el proceso de evaluación de los riesgos de seguridad de la información que permita:

a) establecer y mantener los criterios de los riesgos de seguridad de la información que incluyan:

- 1) Los criterios de aceptación del riesgo; y
- 2) Los criterios para el desempeño de las evaluaciones de los riesgos de la seguridad de la información;

b) Garantizar que la repetición de la evaluación repetitiva de los riesgos de la seguridad de la información arroje resultados válidos, consistentes y comparativos;

c) Identificar los riesgos de seguridad de la información:

1) Aplicando del proceso de evaluación de los riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información; y

2) Identificando a los originadores de los riesgos;

d) Analizar los riesgos de seguridad de la información:

1) Evaluando las consecuencias potenciales que se producirían si los riesgos identificados en el punto 6.1.2 c) 1) llegaran a materializarse;

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

3) Determinando los niveles de riesgo;

e) Evaluar los riesgos de la seguridad de la información:

1) Comparando los resultados del análisis de riesgos con los criterios de riesgos establecidos en el punto 6.1.2 a); y

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

La organización deberá conservar la información documentada acerca del proceso de evaluación de la seguridad de la información.

6. 1. 3 Tratamiento de los riesgos de la seguridad de la Información

La organización deberá definir y aplicar el proceso de tratamiento de los riesgos de la seguridad de la información con la finalidad de:

a) Seleccionar las opciones de tratamiento de los riesgos de seguridad de la información, tomando en cuenta los resultados de la evaluación de los riesgos;

b) Determinar todos los controles que son necesarios para implementar la opción u opciones seleccionadas para el tratamiento de la seguridad de la información;

NOTA: Las organizaciones pueden diseñar los controles según lo requerido o pueden identificarlos desde otras fuentes.

c) Comparar los controles determinados en el punto 6.1.3 b), que anteriormente fueron * determinados en el Anexo A, y verificar que no se haya omitido ningún control que sea de utilidad;

NOTA 1 Anexo A contiene una lista completa de objetivos y mecanismos de control. Los usuarios de esta Norma Internacional se dirigen al Anexo A, para garantizar que no se pase por alto ningún control que sea necesario.

NOTA 2 Los objetivos de control están incluidos de manera implícita en los controles seleccionados. Los * objetivos de control y los mecanismos de control enlistados en el Anexo A no son exhaustivos y se requiere de objetivos de control y controles adicionales.

d) Elaborar una Declaración de Aplicabilidad que contiene los controles necesarios (ver punto 6.1.3 b) y c)) y la argumentación de las inclusiones, si se aplicaran o no, y la argumentación de las exclusiones del control del Anexo A;

e) Formular el tratamiento de los riesgos de seguridad de la información; y

f) Hacer que los poseedores del riesgos aprueben el plan de del tratamiento de riesgos de la seguridad de la información y acepten los riesgos residuales de la seguridad de la información.

La organización deberá conservar la información documentada acerca del proceso de tratamiento de los riesgos de la seguridad de la información

NOTA: La evaluación y el proceso de tratamiento de los riesgos de seguridad de la información se alinea con los principios y lineamientos genéricos proporcionados en ISO 31000[5].

6.2 Objetivos de Seguridad de la Información y la planificación para alcanzarlos

La organización deberá establecer los objetivos de seguridad de la información en relación a las funciones y niveles

Los objetivos de seguridad de la información deberán:

- a) Ser consistentes con la política de seguridad de la información;
- b) Ser medibles (si es aplicable);
- c) Tomar en cuenta los requisitos de la seguridad de la información y los resultados de la evaluación de riesgos y del tratamiento de riesgos;
- d) Ser comunicados; y
- e) Actualizarse, si así lo requiriera.

La organización deberá conservar la información documentada sobre los objetivos de la seguridad de la información. Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización deberá determinar:

- f) Qué deberá hacer;
- g) Qué recursos necesitará;
- h) Quién será el responsable;
- i) Cuándo será alcanzado dicho objetivo; y
- j) Cómo medirá los resultados.

7 Apoyo / Soporte

7.1 Recursos

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

7.2 Competencia

P.Ex. Que significa Personal competente? (E)

La organización:

- a) Determinará la competencia necesaria de la o las personas que harán el trabajo bajo su control, el mismo que afectará el desempeño de su seguridad de la información;
- b) Garantizará que estas personas tengan una competencia en base a una educación, entrenamiento y experiencia adecuados;
- c) Si fuera el caso, llevar a cabo acciones que permitan adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas; y
- d) Conservar una adecuada documentación de la información como evidencia de la competencia

NOTA: Acciones que podrían tomarse, como por ejemplo: capacitación, tutoría o reasignación de empleados actuales; o la contratación o sub contratación de personal competente

7.3 Concientización

Las personas que hacen el trabajo bajo en control de la organización deberán ser conscientes de:

- a) La política de seguridad de la información;
- b) Su contribución a la efectividad del sistema de gestión de la seguridad de la información, incluyendo los beneficios de la mejora en el desempeño de la seguridad de la información; y
- c) Las implicancias de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.

7.4 Comunicación

La organización determinará la necesidad de las comunicaciones internas y externas con respecto al sistema de gestión de la información incluyendo:

- a) Qué se debe comunicar;
- b) Cuándo se debe comunicar;
- c) Con quién se debe comunicar;
- d) Quién debe comunicar; y
- e) El proceso por el cual se debe hacer efectiva la comunicación.

7.5 Documentación de la información

7.5.1 General

El sistema de gestión de la información incluirá:

- a) la documentación de la información requerida por la Norma Internacional; y
- b) La documentación de la información determinada por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.

NOTA: El alcance de la documentación de la información para el sistema de gestión de la seguridad de la información podría diferir de una organización a otra debido a:

- 1) El tamaño de la organización y a su tipo de actividades, procesos, productos y servicios;
- 2) La complejidad de los procesos y sus interacciones; y
- 3) La competencia de las personas.

7.5.2 Creación y actualización

Al crear y actualización la información documentada, la organización deberá garantizar una apropiada:

- a) Identificación y descripción (e.g. un título, fecha, autor o número de referencia);
- b) Formato (e.g. idioma, versión del software, gráficos) y los medios (e.g. papel, electrónico); y
- c) Revisión y aprobación para una debida adecuación e idoneidad.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por la presente Norma Internacional deberá ser controlada para garantizar:

- a) La disponibilidad e idoneidad para su uso, donde y en el momento que sea necesario; y
- b) Su adecuada protección (e.g. de pérdida de confidencialidad, uso inadecuado o pérdida de integridad)

Para el control de la información documentada, la organización deberá desarrollar las siguientes actividades, según corresponda:

- c) Distribución, acceso, recuperación y uso;
- d) Almacenamiento y conservación, incluyendo la conservación de la legibilidad;
- e) Control de cambios (e.g. control de la versión); y
- f) Retención y disposición.

Se deberá identificar y controlar, en la medida de lo posible, la información documentada de origen externo, determinado por la organización como necesaria para la planificación y operación del sistema de gestión de la información.

NOTA: El acceso implica una decisión con respecto al permiso para ver únicamente la información, o el permiso o la autoridad para ver y cambiar la información documentada, etc.

8 Operación

8.1 Planificación y control operacional

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

La organización deberá mantener información documentada de tal forma que garantice que se está llevando a cabo los procesos de acuerdo a lo planificado.

La organización deberá mantener un control sobre los cambios planificados y revisar las consecuencias de los cambios involuntarios, tomando acción para mitigar cualquier efecto adverso, si el caso así lo ameritara.

La organización deberá garantizar identificar y controlar todos los procesos tercerizados.

8.2 Evaluación de los riesgos de seguridad de la información

La organización deberá llevar a cabo evaluaciones de los riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se dan cambios, tomando en cuenta los criterios establecidos en el punto 6.1.2 a).

La organización deberá conservar la información documentada de los resultados de la evaluación de los riesgos de la seguridad de la información.

8.3 Tratamiento de los riesgos de la seguridad de la Información

La organización deberá implementar el plan de tratamiento de los riesgos de seguridad de la información. La organización deberá conservar la información documentada de los resultados del tratamiento de los riesgos de la seguridad de la información.

9 Evaluación del desempeño

9.1 Monitoreo, medición, análisis y evaluación

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

La organización deberá determinar:

- a) Qué necesidades deben ser monitoreadas y sometidas a medición, incluyendo los procesos y controles de la seguridad de la información;
- b) Los métodos de monitoreo, medición, análisis y evaluación, según corresponda, con la finalidad de garantizar la validez de los resultados;

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

- c) Cuándo deberá ejecutarse el monitoreo y la medición;
- d) Quién deberá hacer el monitoreo y la medición;
- e) Cuándo deberán analizarse y evaluarse los resultados del monitoreo y de la medición; y
- f) Quién deberá analizar y evaluar los resultados.

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

9.2 Auditorías internas

La organización deberá dirigir auditorías internas en intervalos planificados con la finalidad de proporcionar información con respecto a que si el sistema de gestión de la seguridad de la información:

- a) Se ajusta a:

- 1) Los propios requisitos de la organización con respecto a su sistema de gestión de la información; y
- 2) Los requisitos de la Norma Internacional

- b) se implementa y mantiene de manera efectiva.

La organización deberá: (E)

- c) Planificar, establecer, implementar y mantener un programa o programas, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y reporte. El o los programas

Documentos para auditoría { - plan de auditoría
(E) { - lista de Verificación

deberán tomar en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

- d) Definir los criterios y alcance de la auditoría;
- e) Seleccionar auditores y dirigir auditorías que aseguren la objetividad e imparcialidad del proceso auditor;
- f) Garantizar que los resultados de la auditoría sean informados a la gerencia correspondiente, y
- g) Conservar información documentada como evidencia del o de los programas y los resultados de la auditoría

9.3 Revisión por parte de la Dirección

La Alta Dirección deberá revisar el sistema de gestión de seguridad de la información a intervalos establecidos para garantizar su continua disponibilidad, adecuación y efectividad

La revisión por parte de la Dirección deberá incluir lo siguiente:

- a) El estatus de las acciones de las anteriores revisiones por parte de la Dirección;
- b) Cambios en los asuntos externos e internos que tuvieron relevancia para el sistema de gestión de la seguridad de la información;
- c) Retroalimentación sobre el desempeño de la seguridad de la información, incluyendo la tendencia en:
 - 1) Las no conformidades y las acciones correctivas;
 - 2) Resultados del monitoreo y medición;
 - 3) Resultados de la auditoría; y
- 4) Cumplimiento de los objetivos de seguridad de la información;
- d) Retroalimentación por parte de las partes interesadas;
- e) Resultados de la evaluación de los riesgos y estatus del plan de tratamiento de los riesgos; y
- f) Oportunidades de mejora continua.

Los resultados de la revisión por parte de la dirección deberán incluir las decisiones con respecto a las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.

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

10 Mejora

P.Ex.) Acción Correctiva ? (E)
Acción Preventiva ?

10.1 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

- a) Reaccionar hacia la no conformidad, y según corresponda:
 - 1) Tomar acción para controlarla y corregirla; y
 - 2) Lidear con las consecuencias;
- b) Evaluar la necesidad de acción para eliminar las causas de la no conformidad, con la finalidad de evitar la recurrencia o la ocurrencia en cualquier otro lugar, mediante:
 - 1) La revisión de la no conformidad;
 - 2) La determinación de las causas de la no conformidad; y
 - 3) La verificación de si existe una no conformidad similar, o podría darse;
 - c) La implementación de una acción necesaria;
 - d) La revisión de la efectividad de las acciones correctivas tomadas; y
 - e) La implementación de cambios al sistema de gestión de la seguridad de la información, si fuera necesario.



Las acciones correctivas deben ser acordes a los efectos de las no conformidades encontradas. La organización deberá conservar la información documentada como evidencia de:

- f) La naturaleza de las no conformidades y cualquier acción tomada posteriormente, y
- g) Los resultados de las acciones correctivas.

10.2 Mejora continua

La organización deberá mejorar de manera continua la idoneidad, adecuación y efectividad del sistema de gestión de la seguridad de la información.

Anexo A (Normativa)

Objetivos de control y controles de referencia

Los objetivos de control y los controles enlistados en el Cuadro A.1 se extraen directamente y están alineados a aquellos detallados en el ISO/IEC 27002:2013[1], Cláusulas del 5 al 18 y deben ser utilizados en el contexto de la Cláusula 6.1.3.

Cuadro A. 1 – Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Gestión de la Gerencia para la seguridad de la información		
A.5.1.1	Políticas de la seguridad de la información	<i>Control</i> La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.
A.5.1.2	Revisión de las políticas de seguridad de la información	<i>Control</i> Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	<i>Control</i> Se debe definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Segregación de tareas	<i>Control</i> Tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activos de la organización.
A.6.1.3	Contacto con las autoridades	<i>Control</i> Se debe mantener contacto adecuado con las autoridades respectivas
A.6.1.4	Contacto con grupos especiales de interés	<i>Control</i> Se debe mantener contacto con grupos especiales de interés u otros forums y asociaciones de profesionales especializados en seguridad
A.6.1.5	Seguridad de la información en la gestión del proyecto	<i>Control</i> La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.
A.6.2 Equipos móviles y trabajo a distancia		
Objetivo: Garantizar la seguridad del trabajo a distancia y del uso de los equipos móviles		
A.6.2.1	Política de los equipos móviles	<i>Control</i> Se debe adoptar políticas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.
A.6.2.2	Trabajo a distancia	<i>Control</i> Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.
A.7 Seguridad de los recursos humanos		
A.7.1. Antes de reclutarlo		
A.7.1.1	Filtración	<i>Control</i> Se debe llevar a cabo la verificación de los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del

		negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.
A.7.1.2	Términos y condiciones del empleo	<p><i>Control</i> Los acuerdos contractuales con los trabajadores y contratistas debe fijar sus responsabilidades y las de la organización con respecto a la seguridad de la información.</p>
A.7.2 Durante el trabajo		
Objetivo: Garantizar que los trabajadores y los contratistas sean conscientes y cumplan con las responsabilidades de la seguridad de la información		
A.7.2.1	Responsabilidades de la Gerencia	<p><i>Control</i> La Gerencia debe instar a todos los trabajadores y contratistas a aplicar la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.</p>
A.7.2.2	Concientización, educación y capacitación sobre seguridad de la información	<p><i>Control</i> Todos los trabajadores de la organización y los contratistas, si así lo requieren, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizacionales, de acuerdo a las funciones de trabajo que desempeñen.</p>
A.7.2.3	Procesos disciplinarios	<p><i>Control</i> Debe haber un proceso disciplinario formal que debe ser comunicado en el lugar, para tomar acción contra los trabajadores que comentan alguna infracción contra la seguridad de la información.</p>
A.7.3 Término y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o término del empleo		
A.7.3.1	Término o cambio de responsabilidades de empleo	<p><i>Control</i> Se debe definir, comunicar y reforzar a todos los trabajadores y contratistas, las responsabilidades y tareas de seguridad de la información que permanecerán válidos después del término del empleo.</p>
A.8 Gestión de los Activos		
A.8.1 Responsabilidades sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades adecuadas de protección		
A.8.1.1	Inventario de activos	<p><i>Control</i> Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos.</p>
A.8.1.2	Propiedad de los activos	<p><i>Control</i> <i>Assets maintained in the inventory shall be owned.</i> Los activos que se encuentren identificados en el inventario deben de ser asignados a un "propietario".</p>
A.8.1.3	Uso aceptable de los activos	<p><i>Control</i> Se debe implementar, documentar e implementar las reglas para el uso aceptable de la información y de los activos relacionados a la información y a las instalaciones de procesamiento de la información.</p>
A.8.1.4	Retorno de los activos	<p><i>Control</i> Todos los trabajadores y usuarios internos y externos deberán devolver todos los activos de la organización que estén en su posesión una vez terminado su empleo, contrato o acuerdo.</p>
A.8.2 Clasificación de la información		
Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización		
A.8.2.1	Clasificación de la información	<p><i>Control</i> La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.</p>
A.8.2.2	Etiquetado de la información	<p><i>Control</i> Se debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la organización.</p>
A.8.2.3	Manejo de los activos	<p><i>Control</i> Se debe desarrollar e implementar procedimientos de manejo de</p>

		los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.
--	--	--

A.8.3 Manejo de los medios de comunicación

Objetivo: Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación

A.8.3.1	Gestión de medios de comunicación removibles	<p><i>Control</i> Se debe implementar procedimientos para la gestión de los medios de comunicación removibles de acuerdo al esquema de clasificación adoptado por la organización</p>
A.8.3.2	Disposición de los medios comunicación	<p><i>Control</i> Los medios comunicación deben ser desechados de manera segura cuando ya no son necesarios, mediante procedimientos formales.</p>
A.8.3.3	Transferencias física de los medios de comunicación	<p><i>Control</i> Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.</p>

A.9 Control de acceso

A.9.1 Requisitos del negocio sobre control del acceso

A.9.1.1	Política de control de acceso	<p><i>Control</i> Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.</p>
A.9.1.2	Acceso a la redes y a los servicios de las redes	<p><i>Control</i> Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.</p>

A.9.2 Gestión del acceso al usuario

Objetivo: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios

A.9.2.1	Registro y des-registro del usuario	<p><i>Control</i> Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso.</p>
A.9.2.2	Provisión de acceso al usuario	<p><i>Control</i> Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.</p>
A.9.2.3	Gestión de los derechos de acceso privilegiado	<p><i>Control</i> Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.</p>
A.9.2.4.	Gestión de información de autenticación secreta de usuarios	<p><i>Control</i> Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.</p>
A.9.2.5	Verificación de los derechos de acceso de los usuarios	<p><i>Control</i> Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.</p>
A.9.2.6	Retiro o ajuste de los derechos de acceso	<p><i>Control</i> Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.</p>

A.9.3 Responsabilidades del usuario

Objetivo: Hacer a los usuarios responsables de salvaguardar la autenticación de su información

A.9.3.1	Uso de información secreta de autenticación	<p><i>Control</i> Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.</p>
---------	---	---

A.9.4 Control de acceso a sistemas y aplicaciones

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

A.9.4.1	Restricción del acceso a la información	<p><i>Control</i> Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.</p>
A.9.4.2	Procedimiento seguro de logeo	<p><i>Control</i> Si así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un</p>

		procedimiento seguro de logeo.
A.9.4.3	Sistema de gestión de la clave	<p><i>Control</i> Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.</p>
A.9.4.4	Uso de programas utilitarios de privilegio	<p><i>Control</i> Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.</p>
A.9.4.5	Control del acceso para programar el código fuente	<p><i>Control</i> Se debe restringir el acceso al programa de código fuente.</p>

A.10 Criptografía

A.10.1 Controles de la criptografía

Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información

A.10.1.1	Política del uso de controles criptográficos	<p><i>Control</i> Se debe desarrollar e implementar una política de uso de controles criptográficos para proteger la información.</p>
A.10.1.2	Gestión de las claves	<p><i>Control</i> Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida.</p>

A.11 Seguridad física y medioambiental

A.11.1 Áreas seguras

Objetivo: Evitar acceso físico no autorizado, daño e interferencia a la información e instalaciones de procesamiento de la información de la organización.

A.11.1.1	Perímetro de seguridad física	<p><i>Control</i> Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.</p>
A.11.1.2	Controles físicos de los ingresos	<p><i>Control</i> Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.</p>
A.11.1.3	Seguridad de las oficinas, salas e instalaciones	<p><i>Control</i> Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.</p>
A.11.1.4	Protección contra las amenazas externas y medioambientales	<p><i>Control</i> Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.</p>
A.11.1.5	Trabajo en áreas seguras	<p><i>Control</i> Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.</p>
A.11.1.6	Distribución de las zonas de carga	<p><i>Control</i> Los puntos de acceso, tales como las zonas de distribución y carga y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible, alejados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.</p>

A.11.2 Equipos

Objetivo: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.

A.11.2.1	Ubicación y protección de los equipos	<p><i>Control</i> Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.</p>
A.11.2.2	Servicios públicos de soporte	<p><i>Control</i> Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.</p>
A.11.2.3	Seguridad en el cableado	<p><i>Control</i> Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.</p>
A.11.2.4	Mantenimiento de los	<p><i>Control</i></p>

	equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de los activos	<i>Control</i> El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización
A.11.2.6	Seguridad de los equipos y bienes fuera de las instalaciones	<i>Control</i> Se debe aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, tomando en cuenta diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Disposición o re-uso seguro de los equipos	<i>Control</i> Todos los equipos que contienen medios de comunicación de la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de desechar o re-usar el mismo.
A.11.2.8	Usuario de equipo abandonado	<i>Control</i> Los usuarios deben garantizar una adecuada protección a los equipos abandonados
A.11.2.9	Política de escritorio y pantallas limpias	<i>Control</i> Se debe adoptar la política de escritorio limpio de papeles y de medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de la información.

A.12 Seguridad de las operaciones

A.12.1 Procedimientos y responsabilidades operaciones

A.12.1.1	Documentación de los procedimientos operacionales	<i>Control</i> Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.
A.12.1.2	Cambios en la gerencia	<i>Control</i> Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información
A.12.1.3	Gestión de la capacidad	<i>Control</i> Debe ser monitoreado y mejorado el uso de recursos, así como las proyecciones hechas sobre los requisitos de capacidad del futuro, para garantizar el desempeño del sistema.
A.12.1.4	Separación de ambientes de desarrollo, prueba y de operaciones	<i>Control</i> Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.

A.12.2 Protección contra el malware (programa malicioso)

Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información estén protegidos contra el malware

A.12.2.1	Controles contra el malware	<i>Control</i> Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al usuario.
----------	-----------------------------	--

A.12.3 Backup

Objetivo: Proteger la información contra la pérdida

A.12.3.1	Backup de la información	<i>Control</i> Se debe tomar y poner a prueba de manera regular, el backup de copias de la información, software e imágenes del sistema, de acuerdo a la política de backup de la organización.
----------	--------------------------	--

A.12.4 Logeo y monitoreo

Objetivo: Registrar eventos y generar evidencias

A.12.4.1	Eventos de logeo	<i>Control</i> Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.
A.12.4.2	Protección de la información del logeo	<i>Control</i> Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo
A.12.4.3	Logeo del administrador y operador	<i>Control</i> Debe logearse las actividades del sistema del administrador y del operador, y los logs deben ser protegidos y revisados de manera regular.
A.12.4.4	Sincronización de los	<i>Control</i>

	relojes	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.
A.12.5 Control del software operacional		
Objetivo: Garantizar la integridad de los sistemas operacionales		
A.12.5.1	Instalación del software en los sistemas operacionales	<p><i>Control</i> Se debe implementar procedimientos para controlar la instalación del software en los sistemas operacionales</p>
A.12.6 Gestión de las vulnerabilidades técnicas		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas		
A.12.6.1	Gestión de las vulnerabilidades técnicas	<p><i>Control</i> Se debe obtener, de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de la información a ser utilizados; evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.</p>
A.12.6.2	Restricciones en la instalación de software	<p><i>Control</i> Se debe establecer e implementar las reglas que gobiernen la instalación de los softwares.</p>
A.12.7 Consideraciones de las auditorías sobre los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de las auditorías en los sistemas operacionales		
A.12.7.1	Controles de la auditoría sobre los sistemas de información	<p><i>Control</i> Se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio</p>
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Garantizar la protección de la información en las redes y de sus instalaciones de procesamiento de la información		
A.13.1.1	Controles en las redes	<p><i>Control</i> Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones</p>
A.13.1.2	Seguridad de los servicios de las redes	<p><i>Control</i> Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.</p>
A.13.1.3	Segregación en las redes	<p><i>Control</i> Se debe separar grupos de servicios de información, usuarios y sistemas de información</p>
A.13.2. Transferencia de la 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 la transferencia de la información	<p><i>Control</i> Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación</p>
A.13.2.2	Acuerdos sobre la transferencias de la información	<p><i>Control</i> Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.</p>
A.13.2.3	Mensajes electrónicos	<p><i>Control</i> Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.</p>
A.13.2.4	Confidencialidad o acuerdos no divulgados	<p><i>Control</i> Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.</p>
A.14.1 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas.		

A.14.1.1	Análisis y especificaciones de los requisitos de la seguridad de la información	<i>Control</i> Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.
A.14.1.2	Seguridad de los servicios de aplicación en las redes públicas	<i>Control</i> Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.
A.14.1.3	Protección de las transacciones de los servicios de aplicación	<i>Control</i> Se debe proteger la información que provenga de las transacciones se los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.
A.14.2 Seguridad en los procesos del programa de desarrollo y soporte		
Objetivo: Garantizar que se diseñe e implemente la seguridad de la información dentro del ciclo del programa de desarrollo de los sistemas de la información		
A.14.2.1	Política del programa de desarrollo seguro	<i>Control</i> Se debe establecer y aplicar reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la organización.
A.14.2.2	Procedimiento de control de los cambios de sistemas	<i>Control</i> Se debe controlar los cambios dentro del ciclo de vida de los programas de desarrollo, mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	<i>Control</i> Luego del cambio de las plataformas operacionales, se debe revisar y verificar las aplicaciones críticas del negocio, para garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.
A.14.2.4	Restricciones a los cambios de los paquetes de software	<i>Control</i> No se facilitará la modificación de los paquetes de sistemas; por el contrario, se les limitará a los cambios necesarios y todos los cambios deberán ser estrictamente controlados.
A.14.2.5	Principios del sistema de seguridad para la ingeniería	<i>Control</i> Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingeniería, a todos los esfuerzos de implementación del sistema.
A.14.2.6	Ambiente seguro del programa de desarrollo	<i>Control</i> Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.
A.14.2.7	Programa de desarrollo subcontratado	<i>Control</i> La organización debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.
A.14.2.8	Revisión de la seguridad del sistema	<i>Control</i> Se debe llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo
A.14.2.9	Revisión de la aceptación del sistema	<i>Control</i> Se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.
A .14.3 Datos de prueba		
Objetivo: garantizar la protección de los datos utilizados para la verificación		
A.14.3.1	Protección de los datos de prueba	<i>Control</i> Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.
A.15 Relación con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Garantizar la protección de los activos de la información a los que los proveedores tiene acceso		
A.15.1.1	Política de seguridad de la información sobre las relaciones con los proveedores	<i>Control</i> Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización.
A.15.1.2	Consideración de la	<i>Control</i>

	seguridad en los acuerdos con los proveedores	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	<p><i>Control</i></p> <p>Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de seguridad de la información relacionados a los servicios de tecnología de la información y la comunicación y a la cadena de suministro del producto.</p>
A.15.2 Gestión de la prestación del servicio por parte del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y de la prestación del servicio alineado a los acuerdos del proveedor		
A.15.2.1	Monitoreo y revisión del servicio de los proveedores	<p><i>Control</i></p> <p>Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.</p>
A.15.2.2	Cambios en la gestión del servicio de los proveedores	<p><i>Control</i></p> <p>Se debe gestionar los cambios a la provisión de los servicios prestados por los proveedores, incluyendo el mantenimiento y la mejora de políticas, procedimientos y controles de la seguridad de la información, tomando en cuenta la sensibilidad de la información del negocio, los sistemas y los procesos involucrados así como la re-evaluación de los riesgos.</p>
A.16 Gestión de los incidentes de seguridad de la información		
A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora		
Objetivo: Garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad		
A.16.1.1	Responsabilidades y procedimientos	<p><i>Control</i></p> <p>Se debe establecer responsabilidades de la gerencia y procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información</p>
A.16.1.2	Reporte de los eventos de seguridad de la información	<p><i>Control</i></p> <p>Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.</p>
A.16.1.3	Reporte de las debilidades de la seguridad de la información	<p><i>Control</i></p> <p>Se debe instar a los trabajadores y contratistas que hagan uso de los sistemas de información de la organización, a tomar nota e informar acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios del sistema de seguridad de la información.</p>
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	<p><i>Control</i></p> <p>Se debe evaluar los eventos de seguridad de la información; y tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.</p>
A.16.1.5	Respuesta a los incidentes de seguridad de la información	<p><i>Control</i></p> <p>Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.</p>
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	<p><i>Control</i></p> <p>Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.</p>
A.16.1.7	Recolección de evidencia	<p><i>Control</i></p> <p>La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.</p>
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización		
A.17.1.1	Continuidad de los planes de seguridad de la información	<p><i>Control</i></p> <p>La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, e.g. durante una crisis o desastre.</p>
A.17.1.2	Implementación de la continuidad de la	<p><i>Control</i></p> <p>La organización deberá establecer, documentar, implementar y</p>

	seguridad de la información	mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	<p><i>Control</i> La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.</p>
A.17.2 Redundancias		
Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de la información		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de la información	<p><i>Control</i> Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.</p>
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y al cualquier requisito de seguridad		
A.18.1.1	Identificación de la ley aplicable y de los requisitos contractuales	<p><i>Control</i> Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información y a la organización.</p>
A.18.1.2	Derechos de propiedad intelectuales	<p><i>Control</i> Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software.</p>
A.18.1.3	Protección de los registros	<p><i>Control</i> Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y lanzamiento no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.</p>
A.18.1.4	Privacidad y protección de la información que permite identificar a las personas	<p><i>Control</i> Se debe garantizar la privacidad y la protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.</p>
A.18.1.5	Regulación de los controles criptográficos	<p><i>Control</i> Se debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.</p>
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Garantizar que la seguridad de la información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales		
A.18.2.1	Revisión independiente de la seguridad de la información	<p><i>Control</i> Se debe revisar, a intervalos planificados o cuando ocurre algún cambio significativo, el enfoque de la organización para gestionar la seguridad de la información y su implementación (i.e. objetivos de control, controles, políticas, procesos y procedimientos de la seguridad de la información).</p>
A.18.2.2	Cumplimiento de las políticas y normas de seguridad de la información	<p><i>Control</i> Los gerentes deben revisar regularmente el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo a las políticas, normas de seguridad adecuadas y a los otros requisitos de seguridad.</p>
A.18.2.3	Revisión del cumplimiento técnico	<p><i>Control</i> Se debe revisar regularmente los sistemas de la información con respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.</p>