NOTA IMPORTANTE:

La entidad sólo puede hacer uso de esta norma para si misma, por lo que este documento NO puede ser reproducido, ni almacenado, ni transmitido, en forma electrónica, fotocopia, grabación o cualquier otra tecnología, fuera de su propio marco.

ININ/ Oficina Nacional de Normalización

NORMA CUBANA

NC

ISO/IEC 27001: 2007
(Publicada por la ISO en 2005)

TECNOLOGÍA DE LA INFORMACIÓN—TÉCNICAS DE SEGURIDAD—SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN—REQUISITOS (ISO/IEC 27001: 2005, IDT)

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

ICS: 35.020

1. Edición Abril 2007
REPRODUCCIÓN PROHIBIDA

Oficina Nacional de Normalización (NC) Calle E No. 261 Vedado, Ciudad de La Habana. Cuba. Teléfono: 830-0835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC), es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información, en el que están representadas las siguientes organizaciones:
  - Ministerio de la Informática y las Comunicaciones
  - SEGURMATICA
  - DESOFT
  - Universidad de las Ciencias Informáticas (UCI)
  - Universidad de Villa Clara
  - Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMATEL)
  - Instituto Superior Politécnico José A. Echeverría
  - Ministerio de Salud Pública (Centro de Control Estatal de Equipos Médicos)
  - Oficina de Seguridad de las Redes Informáticas
  - Oficina Nacional de Normalización
- Es una adopción idéntica por el método de traducción de la Norma Internacional ISO/IEC 27001:2005 *Information technology — Security techniques — Information security management systems — Requirements*

© NC, 2007

Todos los derechos reservados. A menos que se especifique, ninguna parte de esta publicación podrá ser reproducida o utilizada en alguna forma o por medios electrónicos o mecánicos, incluyendo las fotocopias, fotografías y microfilmes, sin el permiso escrito previo de:
Oficina Nacional de Normalización (NC)
Calle E No. 261, Vedado, Ciudad de La Habana, Habana 4, Cuba.

Impreso en Cuba.

Índice

Prefacio de la Norma

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los órganos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

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

La tarea principal del comité técnico conjunto es la de preparar normas internacionales. Los borradores de normas internacionales adoptadas por el Comité Técnico Conjunto son circulados a los organismos nacionales para su voto. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos nacionales.

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

La Norma Internacional ISO/IEC 27001 fue preparada por el Comité Técnico Conjunto ISO/IEC JTC1, *Tecnología de la Información*, subcomité SC 27, *Técnicas de seguridad en TI.*

0 Introducción

0.1 Generalidades

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas.

0.2 Enfoque basado en procesos

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.

Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos”.

El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a sus usuarios a hacer énfasis en la importancia de:

a) comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;

b) implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;

c) realizar el seguimiento y revisión del desempeño y eficacia del SGSI; y

d) la mejora continua basada en la medición de objetivos.

Esta norma adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI. La Figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. La Figura 1 también ilustra los vínculos en los procesos especificados en los apartados 4, 5, 6, 7 y 8.

La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002)[1] que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

EJEMPLO 1

Un requisito podría ser que las violaciones a la seguridad de la información no causen daño financiero severo a una organización, ni sean motivo de preocupación para ésta.

EJEMPLO 2

Una expectativa podría ser que si ocurre un incidente serio, como por ejemplo el *hacking* del sitio Web de una organización, haya personas con capacitación suficiente en los procedimientos apropiados, para minimizar el impacto.

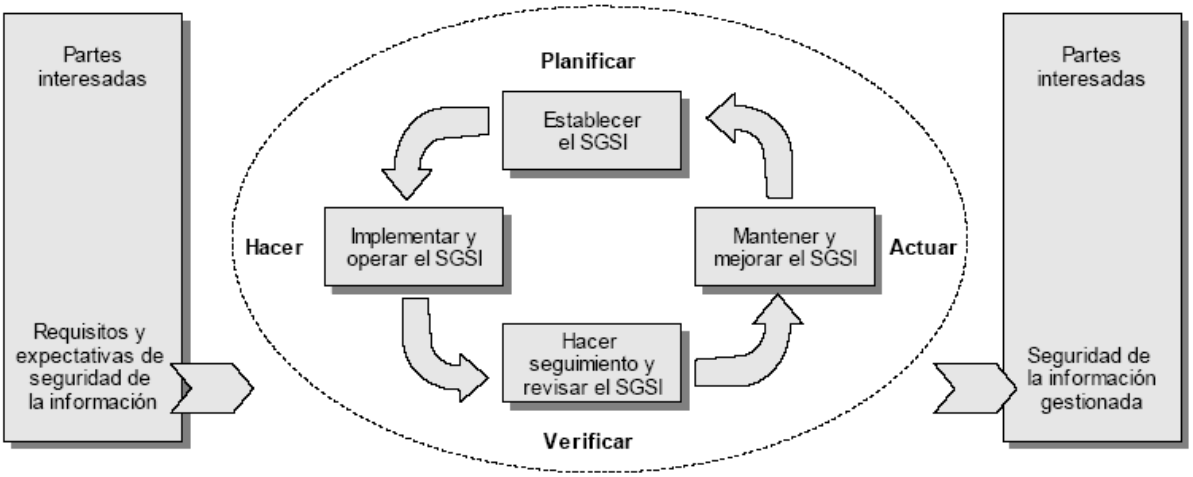

Figura 1. Modelo PHVA aplicado a los procesos de SGSI

Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

[1] Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002. www.oecd.org.

0.3 Compatibilidad con otros sistemas de gestión

Esta norma está alineada con la ISO 9001:2000 y la ISO 14001:2004, con el fin de apoyar la implementación y operación, consistentes e integradas con normas de gestión relacionadas. Un sistema de gestión diseñado adecuadamente puede entonces satisfacer los requisitos de todas estas normas. La Tabla C.1 ilustra la relación entre los apartados de esta norma, la norma ISO 9001:2000 y la ISO 14001:2004.

Esta norma está diseñada para permitir a una organización alinear o integrar su SGSI con los requisitos de los sistemas de gestión relacionados.

TECNOLOGÍA DE LA INFORMACIÓN— TÉCNICAS DE SEGURIDAD—SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN—REQUISITOS

IMPORTANTE - Ésta publicación no pretende incluir todas las disposiciones necesarias de un contrato. Los usuarios son responsables de su correcta aplicación. El cumplimiento con una norma en sí misma no confiere exención de las obligaciones legales.

1 – Objeto

1.1 Generalidades

Esta norma cubre todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas.

El SGSI se diseña para asegurar la selección de controles de seguridad adecuados y proporcionados que protejan los activos de información y brinden confianza a las partes interesadas.

NOTA 1 Las referencias que se hacen en esta norma a “negocio” se deberían interpretar ampliamente como aquellas actividades que son esenciales para la existencia de la organización.

NOTA 2 La ISO/IEC 17799 brinda orientación sobre la implementación, que se puede usar cuando se diseñan controles.

1.2 Aplicación

Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza. No es aceptable la exclusión de cualquiera de los requisitos especificados en los apartados 4, 5, 6, 7 y 8 cuando una organización declara conformidad con la presente norma.

Cualquier exclusión de controles, considerada necesaria para satisfacer los criterios de aceptación de riesgos, necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados por las personas responsables. En donde se excluya cualquier control, las declaraciones de conformidad con esta norma no son aceptables a menos que dichas exclusiones no afecten la capacidad de la organización y/o la responsabilidad para ofrecer seguridad de la información que satisfaga los requisitos de seguridad determinados por la evaluación de riesgos y los requisitos reglamentarios aplicables.

NOTA Si una organización ya tiene en funcionamiento un sistema de gestión de los procesos de su negocio (por ejemplo: en relación con la ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requisitos de la presente norma dentro de este sistema de gestión existente.

2 –Referencias normativas

Los siguientes documentos referenciados son indispensables para la aplicación de esta norma. Para las referencias fechadas, sólo se aplica la edición citada. Para las referencias no fechadas, se aplica la última edición del documento referenciado (incluida cualquier corrección).

ISO/IEC 17799:2005, *Information Technology. Security Techniques. Code of Practice for Information Security Management.*

3 –Términos y definiciones

Para los propósitos de esta norma, se aplican los siguientes términos y definiciones:

3.1
activo
aquello que tenga valor para la organización.
[ISO/IEC 13335-1:2004]

3.2
disponibilidad
propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
[ISO/IEC 13335-1:2004]

3.3
confidencialidad
propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
[ISO/IEC 13335-1:2004]

3.4
seguridad de la información
preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (*accountability*), no repudio y confiabilidad.
[ISO/IEC 17799:2005]

3.5
evento de seguridad de la información
ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.
[ISO/IEC TR 18044:2004]

3.6
incidente de seguridad de la información
un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
[ISO/IEC TR 18044:2004]

3.7
sistema de gestión de la seguridad de la información
SGSI
parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

NOTA El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

3.8
integridad
propiedad de salvaguardar la exactitud y estado completo de los activos.
[ISO/IEC 13335-1:2004]

3.9
riesgo residual
nivel restante de riesgo después del tratamiento del riesgo.
[Guía ISO/IEC 73:2002]

3.10
aceptación del riesgo
decisión de asumir un riesgo.
[Guía ISO/IEC 73:2002]

3.11
análisis de riesgo
uso sistemático de la información para identificar las fuentes y estimar el riesgo.
[Guía ISO/IEC 73:2002]

3.12
evaluación del riesgo
proceso global de análisis y evaluación del riesgo.
[Guía ISO/IEC 73:2002]

3.13
valoración del riesgo
proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
[Guía ISO/IEC 73:2002]

3.14
gestión del riesgo
actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
[Guía ISO/IEC 73:2002]

3.15
tratamiento del riesgo
proceso de selección e implementación de medidas para modificar el riesgo.
[Guía ISO/IEC 73:2002]

NOTA En la presente norma el término “control” se usa como sinónimo de “medida”.

3.16
declaración de aplicabilidad
documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

NOTA Los objetivos de control y los controles se basan en los resultados y conclusiones de los procesos de evaluación y tratamiento de riesgos, requisitos legales o reglamentarios, obligaciones contractuales y los requisitos del negocio de la organización en cuanto a la seguridad de la información.

4 - Sistema de gestión de la seguridad de la información

4.1 Requisitos generales

La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta. Para los propósitos de esta norma, el proceso usado se basa en el modelo PHVA que se ilustra en la Figura 1.

4.2 Establecimiento y gestión del SGSI

4.2.1 Establecimiento del SGSI

La organización debe:

a) Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance (véase el apartado 1.2).

b) Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que:

1) incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información;

2) tenga en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales;

3) esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI;

4) establezca los criterios contra los cuales se evaluará el riesgo. (véase el apartado 4.2.1, literal c) y;

5) haya sido aprobada por la dirección.

NOTA: En cuanto a los propósitos de esta norma, la política de seguridad de la información se considera un subconjunto de la política del SGSI. Estas políticas pueden describirse en un documento.

c) Definir el enfoque organizacional para la evaluación del riesgo.

1) Identificar una metodología de evaluación del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.

2) Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables. (véase el apartado 5.1, literal f).

La metodología seleccionada para evaluación de riesgos debe asegurar que dichas evaluaciones producen resultados comparables y reproducibles.

NOTA Existen diferentes metodologías para la evaluación de riesgos. En el documento ISO/IEC TR 13335-3, *Information technology. Guidelines for the Management of IT Security – Techniques for the Management of IT Security* se presentan algunos ejemplos:

d) Identificar los riesgos

1) identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos;

2) identificar las amenazas a estos activos;

3) identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas;

4) Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

e) Analizar y evaluar los riesgos

1) evaluar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos;

2) evaluar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente;

3) estimar los niveles de los riesgos;

4) determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios establecidos en el apartado 4.2.1, literal c).

f) Identificar y evaluar las opciones para el tratamiento de los riesgos.

Las posibles acciones incluyen:

1) aplicar los controles apropiados;

2) aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos (véase el apartado 4.2.1,literal c);

3) evitar riesgos, y

4) transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc.

[2] El término “propietario” no quiere decir que la persona realmente tenga algún derecho de propiedad sobre el activo. Anexo A como punto de partida para la selección de controles, con el fin de asegurarse de que no se pasan por alto opciones de control importantes.

g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de evaluación y tratamiento de riesgos. Esta selección debe tener en cuenta los criterios para la aceptación de riesgos (véase el apartado 4.2.1. literal c), al igual que los requisitos legales, reglamentarios y contractuales.

Los objetivos de control y los controles del Anexo A se deben seleccionar como parte de este proceso, en tanto sean adecuados para cubrir estos requisitos.

Los objetivos de control y los controles presentados en el Anexo A no son exhaustivos, por lo que puede ser necesario seleccionar objetivos de control y controles adicionales.

NOTA El Anexo A contiene una lista amplia de objetivos de control y controles que comúnmente se han encontrado pertinentes en las organizaciones. Se sugiere a los usuarios de esta norma consultar la NOTA 2.

h) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

i) Obtener autorización de la dirección para implementar y operar el SGSI.

j) Elaborar una declaración de aplicabilidad.

Se debe elaborar una declaración de aplicabilidad que incluya:

1) Los objetivos de control y los controles, seleccionados en el apartado 4.2.1, literal g) y las razones para su selección.

2) Los objetivos de control y los controles implementados actualmente (véase el apartado 4.2.1., literal e) 2)), y

3) La exclusión de cualquier objetivo de control y controles enumerados en el Anexo A y la justificación para su exclusión.

NOTA La declaración de aplicabilidad proporciona un resumen de las decisiones concernientes al tratamiento de los riesgos. La justificación de las exclusiones permite validar que ningún control se omita involuntariamente.

4.2.2 Implementación y operación del SGSI

La organización debe:

a) Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información (véase el apartado 5).

b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en el apartado 4.2.1, literal g) para cumplir los objetivos de control.

d) Definir cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de evaluar la eficacia de los controles para producir resultados comparables y reproducibles (véase el apartado 4.2.3 literal c).

NOTA La medición de la eficacia de los controles permite a los gerentes y al personal determinar la medida en que se cumplen los objetivos de control planificados.

e) Implementar programas de formación y de toma de conciencia, (véase el apartado 5.2.2).

f) Gestionar la operación del SGSI.

g) Gestionar los recursos del SGSI (véase el apartado 5.2).

h) Implementar procedimientos y otros controles para detectar rápidamente y dar respuesta oportuna a los incidentes de seguridad (véase el apartado 4.2.3).

4.2.3 Seguimiento y revisión del SGSI

La organización debe:

a) Ejecutar procedimientos de seguimiento y revisión y otros controles para:

1) detectar rápidamente errores en los resultados del procesamiento;

2) identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron;

3) posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están desempeñando en la forma esperada;

4) ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores, y

5) determinar si las acciones tomadas para solucionar una brecha de seguridad fueron eficaces.

b) Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

d) Revisar las evaluaciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:

1) la organización,

2) la tecnología,

3) los objetivos y procesos del negocio,

4) las amenazas identificadas,

5) la eficacia de los controles implementados, y

6) eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.

e) Realizar auditorías internas del SGSI a intervalos planificados (véase el apartado 6).

NOTA Las auditorías internas, denominadas algunas veces auditorías de primera parte, las realiza la propia organización u otra organización en su nombre, para propósitos internos.

f) Emprender una revisión del SGSI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de SGSI (véase el apartado 7.1).

g) Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.

h) Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI (véase el apartado 4.3.3).

4.2.4 Mantenimiento y mejora del SGSI

La organización debe, regularmente:

a) Implementar las mejoras identificadas en el SGSI;

b) Emprender las acciones correctivas y preventivas adecuadas de acuerdo con los apartados 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización;

c) Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, y en donde sea pertinente, llegar a acuerdos sobre cómo proceder;

d) Asegurar que las mejoras logran los objetivos previstos.

4.3 Requisitos de documentación

4.3.1 Generalidades

La documentación del SGSI debe incluir registros de las decisiones de la dirección, asegurar que las acciones sean trazables a las decisiones y políticas de la gerencia, y que los resultados registrados sean reproducibles.

Es importante ser capaz de demostrar la relación entre los controles seleccionados y los resultados del proceso de evaluación y tratamiento de riesgos, y seguidamente, con la política y objetivos del SGSI.

La documentación del SGSI debe incluir:
a) declaraciones documentadas de la política y objetivos del SGSI (véase el apartado 4.2.1, literal b));

b) el alcance del SGSI (véase el apartado 4.2.1, literal a));

c) los procedimientos y controles que apoyan el SGSI;

d) una descripción de la metodología de evaluación de riesgos (véase el apartado 4.2.1, literal c));

e) el informe de evaluación de riesgos (véase el apartado 4.2.1. literales c) a g));

f) el plan de tratamiento de riesgos (véase el apartado 4.2.2, literal b));

g) los procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles (véase el apartado 4.2.3. literal c));

h) los registros exigidos por esta norma (véase el apartado 4.3.3); y

i) la Declaración de Aplicabilidad.

NOTA 1 En esta norma, el término “procedimiento documentado” significa que el procedimiento está establecido, documentado, implementado y mantenido.

NOTA 2 El alcance de la documentación del SGSI puede ser diferente de una organización a otra debido a:

- El tamaño de la organización y el tipo de sus actividades, y
- El alcance y complejidad de los requisitos de seguridad y del sistema que se está gestionando.

NOTA 3 Los documentos y registros pueden tener cualquier forma o estar en cualquier tipo de medio.

4.3.2 Control de documentos

Los documentos exigidos por el SGSI se deben proteger y controlar. Se debe establecer un procedimiento documentado para definir las acciones de gestión necesarias para:

a) aprobar los documentos en cuanto a su adecuación antes de su publicación;

b) revisar y actualizar los documentos según sea necesario y reaprobarlos;

c) asegurar que los cambios y el estado de actualización de los documentos estén identificados;

d) asegurar que las versiones más recientes de los documentos pertinentes están disponibles en los puntos de uso;

e) asegurar que los documentos permanezcan legibles y fácilmente identificables;

f) asegurar que los documentos estén disponibles para quienes los necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su transferencia, almacenamiento y disposición final;

g) asegurar que los documentos de origen externo estén identificados;

h) asegurar que la distribución de documentos esté controlada;

i) impedir el uso no previsto de los documentos obsoletos; y

j) aplicar la identificación adecuada a los documentos obsoletos, si se retienen para cualquier propósito.

4.3.3 Control de registros

Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros deben estar protegidos y controlados.

El SGSI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros se deben documentar e implementar.

Se deben llevar registros del desempeño del proceso, como se esboza en el apartado 4.2, y de todos los casos de incidentes de seguridad significativos relacionados con el SGSI.

EJEMPLO Algunos ejemplos de registros son: un libro de visitantes, informes de auditorías y formatos de autorización de acceso diligenciados.

5 - Responsabilidad de la dirección

5.1 Compromiso de la dirección

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI:

a) mediante el establecimiento de una política del SGSI;

b) asegurando que se establezcan los objetivos y planes del SGSI;

c) estableciendo funciones y responsabilidades de seguridad de la información;

d) comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua;

e) brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI (véase el apartado 5.2.1);

f) decidiendo los criterios para aceptación de riesgos, y los niveles de riesgo aceptables;

g) asegurando que se realizan auditorías internas del SGSI (véase el apartado 6); y

h) efectuando las revisiones por la dirección, del SGSI (véase el apartado 7).

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y suministrar los recursos necesarios para:

a) establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI;

b) asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio;

c) identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;

d) mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;

e) llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente a los resultados de estas revisiones; y

f) en donde se requiera, mejorar la eficacia del SGSI.

5.2.2 Formación, toma de conciencia y competencia

La organización debe asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI sea competente para realizar las tareas exigidas, mediante:

a) la determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el SGSI;

b) el suministro de formación o realización de otras acciones (por ejemplo, la contratación de personal competente) para satisfacer estas necesidades;

c) la evaluación de la eficacia de las acciones emprendidas, y

d) el mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones (véase el apartado 4.3.3).

La organización también debe asegurar que todo el personal apropiado tiene conciencia de la pertinencia e importancia de sus actividades de seguridad de la información y cómo ellas contribuyen al logro de los objetivos del SGSI.

6 - Auditorias internas del SGSI

La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI:

a) cumplen los requisitos de la presente norma y de la legislación o reglamentaciones pertinentes;

b) cumplen los requisitos identificados de seguridad de la información;

c) están implementados y se mantienen eficazmente, y

d) tienen un desempeño acorde con lo esperado.
Se debe planificar un programa de auditorías tomando en cuenta el estado e importancia de los procesos y las áreas que se van a auditar, así como los resultados de las auditorías previas. Se deben definir los criterios, el alcance, la frecuencia y los métodos de la auditoría.

La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Se deben definir en un procedimiento documentado las responsabilidades y requisitos para la planificación y realización de las auditorías, para informar los resultados, y para mantener los registros (véase el apartado 4.3.3).

La dirección responsable del área auditada debe asegurarse de que las acciones para eliminar las no conformidades detectadas y sus causas, se emprendan sin demora injustificada. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de la verificación.

NOTA La norma ISO 19011:2002, Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiente puede brindar orientación útil para la realización de auditorías internas del SGSI.

7 - Revisión del SGSI por la dirección

7.1 Generalidades

La dirección debe revisar el SGSI de la organización a intervalos planificados (por lo menos una vez al año), para asegurar su conveniencia, suficiencia y eficacia continuas. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros (véase el apartado 4.3.3).

7.2 Información para la revisión

Las entradas para la revisión por la dirección deben incluir:

a) resultados de las auditorías y revisiones del SGSI;

b) retroalimentación de las partes interesadas;

c) técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del SGSI;

d) estado de las acciones correctivas y preventivas;

e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación previa de los riesgos;

f) resultados de las mediciones de eficacia;

g) acciones de seguimiento resultantes de revisiones anteriores por la dirección;

h) cualquier cambio que pueda afectar el SGSI; y

i) recomendaciones para mejoras.

7.3 Resultados de la revisión

Los resultados de la revisión por la dirección deben incluir cualquier decisión y acción relacionada con:

a) La mejora de la eficacia del SGSI.

b) La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.

c) La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que pueden tener impacto en el SGSI, incluidos cambios a:

1) los requisitos del negocio;

2) los requisitos de seguridad;

3) los procesos del negocio que afectan los requisitos del negocio existentes;

4) los requisitos reglamentarios o legales;

5) las obligaciones contractuales; y

6) los niveles de riesgo y/o niveles de aceptación de riesgos.

d) Los recursos necesarios.

e) La mejora a la manera en que se mide la eficacia de los controles.

8 - Mejora del SGSI
8.1 Mejora continua

La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de seguridad de la información, los resultados de la auditoría, el análisis de los eventos a los que se les ha hecho seguimiento, las acciones correctivas y preventivas y la revisión por la dirección.

8.2 Acción correctiva

La organización debe emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente. El procedimiento documentado para la acción correctiva debe definir requisitos para:

a) identificar las no conformidades;

b) determinar las causas de las no conformidades;

c) evaluar la necesidad de acciones que aseguren que las no conformidades no vuelven a ocurrir;
d) determinar e implementar la acción correctiva necesaria;

e) registrar los resultados de la acción tomada (véase el apartado 4.3.3); y

f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar acciones para eliminar la causa de no conformidades potenciales con los requisitos del SGSI y evitar que ocurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir requisitos para:

a) identificar no conformidades potenciales y sus causas;

b) evaluar la necesidad de acciones para impedir que las no conformidades ocurran;

c) determinar e implementar la acción preventiva necesaria;

d) registrar los resultados de la acción tomada (véase el apartado 4.3.3), y

e) revisar la acción preventiva tomada.

La organización debe identificar los cambios en los riesgos e identificar los requisitos en cuanto acciones preventivas, concentrando la atención en los riesgos que han cambiado significativamente.

La prioridad de las acciones preventivas se debe determinar basada en los resultados de la evaluación de riesgos.

NOTA Las acciones para prevenir no conformidades con frecuencia son más rentables que la acción correctiva.

ANEXO A
(Normativo)

OBJETIVOS DE CONTROL Y CONTROLES

Los objetivos de control y los controles enumerados en la Tabla A.1 se han obtenido directamente de los de la ISO/IEC 17799:2005, apartados 5 a 15, y están alineados con ellos.

Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas se deben seleccionar como parte del proceso de SGSI especificado en el apartado 4.2.1.

La norma ISO/IEC 17799:2005, apartados 5 a 15, proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados en el literal A.5 a A.15.

Tabla A.1. Objetivos de control y controles

A.5 POLÍTICA DE SEGURIDAD		
A.5.1 Política de seguridad de la información *Objetivo:* Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.		
A.5.1.1	Documento de política de seguridad de la información	*Control* La dirección debe aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes, un documento con la política de seguridad de la información.
A.5.1.2	Revisión de la política de seguridad de la información	*Control* Se debe revisar la política de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización interna *Objetivo:* Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la dirección con la seguridad de la información	*Control* La dirección debe apoyar activamente la seguridad dentro de la organización a través de una orientación clara, compromiso demostrado, y la asignación explícita de las responsabilidades de seguridad de la información y su reconocimiento.
A.6.1.2	Coordinación de la seguridad de la información	*Control* Las actividades referentes a la seguridad de la información deben estar coordinadas por representantes de diferentes partes de la organización con funciones y roles pertinentes.
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	*Control* Se deben definir claramente todas las responsabilidades de seguridad de la información.
A.6.1.4	Proceso de autorización para las instalaciones de procesamiento de información	*Control* Se debe definir e implementar un proceso de autorización por parte de la dirección para nuevas instalaciones de procesamiento de información.

A.6.1.5	Acuerdos de confidencialidad	*Control* Se deben identificar y revisar regularmente los requisitos sobre acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	*Control* Se deben mantener contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	*Control* Se deben mantener los contactos apropiados con los grupos de interés especial u otros foros especializados en seguridad, así como asociaciones de profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.
A.6.2 Partes externas *Objetivo:* Mantener la seguridad de la información de la organización y de las instalaciones de procesamiento de información a las que tienen acceso las partes externas, o que son procesadas, comunicadas o gestionadas por éstas.		
A.6.2.1	Identificación de los riesgos relacionados con partes externas	*Control* Se deben identificar los riesgos asociados a la información de la organización y a las instalaciones de procesamiento de la información para los procesos de negocio que involucran partes externas, y deberían implementarse controles apropiados antes de otorgar el acceso.
A.6.2.2	Tener en cuenta la seguridad cuando se trata con clientes	*Control* Todos los requisitos de seguridad identificados se deben tratar antes de brindarles a los clientes acceso a activos o información de la organización.
A.6.2.3	Tener en cuenta la seguridad en los acuerdos con terceras partes	*Control* Los acuerdos con terceros que involucren acceso, procesamiento, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información, o el agregado de productos o servicios a las instalaciones de procesamiento de información, deben cubrir todos los requisitos de seguridad pertinentes.
A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad sobre los activos *Objetivo:* Implementar y mantener una adecuada protección sobre los activos de la organización.		
A.7.1.1	Inventario de activos	*Control* Todos los activos se deben identificar claramente y se debe elaborar y mantener un inventario de todos los activos importantes.

A.7.1.2	Propiedad de los activos	*Control* Toda la información y activos asociados con las instalaciones de procesamiento de información deben pertenecer a un "propietario[3]", designado por la organización.
A.7.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar las reglas para el uso aceptable de información y activos asociados con las instalaciones de procesamiento de información
A.7.2 Clasificación de la información *Objetivo:* Asegurar que la información recibe el nivel de protección adecuado.		
A.7.2.1	Directrices de clasificación	*Control* La información se debe clasificarse en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	Etiquetado y manejo de la información	*Control* Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
A.8.1 Previo al empleo[4] *Objetivo:* asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados, y para reducir el riesgo de hurto, fraude o mal uso de las instalaciones.		
A.8.1.1	Roles y responsabilidades	*Control* Los roles y responsabilidades de seguridad de usuarios empleados, contratistas y de terceras partes se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.
A.8.1.2	Selección	*Control* Debe realizarse la verificación de antecedentes en todos los candidatos al empleo, contratistas, y usuarios de terceras partes de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.
A.8.1.3	Términos y condiciones de la relación laboral	*Control* Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben acordar y firmar los términos y condiciones de su contrato laboral, el cual debe indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.

[3] Explicación: El término "propietario" identifica un individuo o entidad que ha probado habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo. El término "propietario" no significa que la persona tiene efectivamente derechos de propiedad sobre el activo.

[4] Explicación: La palabra "empleo" busca cubrir las siguientes situaciones diferentes: empleo de personal (temporal o de mayor duración), asignación y cambio de roles de trabajo, asignación de contratos, y la finalización de estos acuerdos.

A.8.2 Durante el empleo *Objetivo:* asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y la pertinencia de la seguridad de la información, de sus responsabilidades y obligaciones, y estén equipados para sustentar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de errores humanos.		
A.8.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a los empleados, contratistas y usuarios de terceras partes aplicar la seguridad de acuerdo con las políticas y procedimientos establecidos por la organización.
A.8.2.2	Concientización, educación y formación en seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas y usuarios de terceras partes, deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal para empleados que han perpetrado una violación a la seguridad.
A.8.3 Finalización o cambio de la relación laboral o empleo *Objetivo:* asegurar que los empleados, contratistas o usuarios de terceras partes se desvinculen de una organización o cambien su relación laboral de una forma ordenada.		
A.8.3.1	Responsabilidades en la desvinculación	*Control* Se deben definir y asignar claramente las responsabilidades relativas a la desvinculación o al cambio de relación laboral.
A.8.3.2	Devolución de activos	*Control* Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.
A.8.3.3	Remoción de derechos de acceso	*Control* Los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información deben ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia.
A.9 SEGURIDAD FÍSICA Y DEL AMBIENTE		
A.9.1 Áreas seguras *Objetivo:* evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta o recepcionista) para proteger las áreas que contienen información e instalaciones de procesamiento de información.
A.9.1.2	Controles de acceso físico	*Control* Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que sólo se permite el acceso a personal autorizado.

A.9.1.3	Seguridad de oficinas, despachos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, despachos e instalaciones.
A.9.1.4	Protección contra amenazas externas y del ambiente	*Control* Se debe diseñar y aplicar medios de protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otras formas de desastre natural o artificial.
A.9.1.5	El trabajo en las áreas seguras	*Control* Se debe diseñar y aplicar protección física y directrices para trabajar en áreas seguras.
A.9.1.6	Áreas de de acceso público, de entrega y de carga	*Control* Los puntos de acceso tales como áreas de entrega y de cargamento y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones deben controlarse, y si es posible, aislarlos de instalaciones de procesamiento de la información para evitar el acceso no autorizado.
A.9.2 Seguridad del equipamiento *Objetivo:* prevenir pérdidas, daños, hurtos o comprometer los activos así como la interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección del equipamiento	*Control* El equipamiento debe ubicarse o protegerse para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
A.9.2.2	Elementos de soporte	*Control* Debe protegerse el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causados por fallas en elementos de soporte.
A.9.2.3	Seguridad en el cableado	*Control* Debe protegerse contra interceptación o daños el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información.
A.9.2.4	Mantenimiento del equipamiento	*Control* El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.
A.9.2.5	Seguridad del equipamiento fuera de las instalaciones de la organización	*Control* Debe asegurarse todo el equipamiento fuera de los locales de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en la reutilización o eliminación de equipos	*Control* Todos aquel equipamiento que contenga medios de almacenamiento debe revisarse para asegurar que todo los datos sensibles y software licenciado se haya removido o se haya sobrescrito con seguridad antes de su disposición.
A.9.2.7	Retiro de bienes	*Control* El equipamiento, la información o el software no deben retirarse del local de la organización sin previa autorización.

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A.10.1 Procedimientos operacionales y responsabilidades *Objetivo:* asegurar la operación correcta y segura de las instalaciones de procesamiento de información.		
A.10.1.1	Procedimientos documentados de operación	*Control* Los procedimientos de operación deben documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambios	*Control* Deben controlarse los cambios en los sistemas e instalaciones de procesamiento de información.
A.10.1.3	Segregación de tareas	*Control* Deben segregarse las tareas y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.
A.10.1.4	Separación de los recursos para desarrollo, prueba y producción	*Control* Los recursos para desarrollo, prueba y producción deben separarse para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.
A.10.2 Gestión de la entrega del servicio por terceras partes *Objetivo:* implementar y mantener un nivel apropiado de la seguridad de la información y la entrega del servicio, acorde con los acuerdos de entrega del servicio por terceras partes.		
A.10.2.1	Entrega del servicio	*Control* Deben asegurarse que los controles de seguridad, las definiciones del servicio y los niveles de entrega incluidos en el acuerdo de entrega del servicio por terceras partes son implementados, operados, y mantenidos por las terceras partes.
A.10.2.2	Supervisión y revisión de los servicios por terceras partes	*Control* Deben supervisarse y revisarse regularmente los servicios, informes y registros proporcionados por las terceras partes, y deben realizarse regularmente auditorías.
A.10.2.3	Gestión de cambios en los servicios de terceras partes	*Control* Los cambios a la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de la seguridad de la información, procedimientos y controles, deben gestionarse tomando en cuenta la importancia de los sistemas y procesos de negocio que impliquen una nueva valoración de riesgos.
A.10.3 Planificación y aceptación del sistema *Objetivo:* minimizar el riesgo de fallos de los sistemas.		
A.10.3.1	Gestión de la capacidad	*Control* Debe supervisarse y adaptarse el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

A.10.3.2	Aceptación del sistema	*Control* Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones, y se deben llevar a cabo las pruebas adecuados del sistema, durante el desarrollo y antes de su aceptación.
A.10.4 Protección contra código malicioso y código móvil *Objetivo:* proteger la integridad del software y la información.		
A.10.4.1	Controles contra código malicioso	*Control* Deben implantarse controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto a procedimientos adecuados para concientizar a los usuarios.
A.10.4.2	Controles contra código móvil	*Control* Donde el uso de código móvil está autorizado, la configuración debe asegurar que el código móvil autorizado opera de acuerdo con una política de seguridad definida, y debe evitarse la ejecución de código móvil no autorizado.
A.10.5 Respaldo *Objetivo:* mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información.		
A.10.5.1	Respaldo de la información	*Control* Deben hacerse regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo.
A.10.6 Gestión de la seguridad de red *Objetivo:* asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	*Control* Las redes deben gestionarse y controlarse adecuadamente, para protegerlas contra amenazas, y mantener la seguridad de los sistemas, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	*Control* Las características de la seguridad, los niveles del servicio, y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en cualquier acuerdo de servicios de red.
A.10.7 Manejo de los medios *Objetivo:* evitar divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio.		
A.10.7.1	Gestión de los medios removibles	*Control* Debe haber implementados procedimientos para la gestión de los medios removibles.
A.10.7.2	Eliminación de los medios	*Control* Deben eliminarse los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.
A.10.7.3	Procedimientos para el manejo de la información	*Control* Deben establecerse procedimientos de utilización y almacenamiento de la información para protegerla de su mal uso o divulgación no autorizada.

A.10.7.4	Seguridad de la documentación de sistemas	*Control* La documentación de sistemas debe protegerse contra el acceso no autorizado.
A.10.8 Intercambio de información *Objetivo:* mantener la seguridad de la información y software intercambiado dentro de una organización y con cualquier otra entidad.		
A.10.8.1	Políticas y procedimientos para intercambio de información	*Control* Deben implementarse políticas formales de intercambio, procedimientos y controles para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación.
A.10.8.2	Acuerdos de intercambio	*Control* Se deben establecer acuerdos para el intercambio de información y de software entre la organización y partes externas.
A.10.8.3	Medios físicos en tránsito	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte más allá de los límites físicos de la organización.
A.10.8.4	Mensajería electrónica.	*Control* La información involucrada en la mensajería electrónica se debe proteger apropiadamente.
A.10.8.5	Sistemas de información de negocio	*Control* Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de negocio.
A.10.9 Servicios de comercio electrónico *Objetivo:* asegurar la seguridad de los servicios de comercio electrónico, así como su uso seguro.		
A.10.9.1	Comercio electrónico	*Control* La información involucrada en el comercio electrónico sobre redes públicas debe ser protegida ante actividades fraudulentas, disputas contractuales, y su divulgación o modificación no autorizada.
A.10.9.2	Transacciones en línea	*Control* La información implicada en transacciones en línea debe protegerse para prevenir la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.
A.10.9.3	Información accesible públicamente	*Control* Debe protegerse la integridad de la información de un sistema accesible públicamente, para prevenir la modificación no autorizada.
A.10.10 Seguimiento *Objetivo:* detectar actividades de procesamiento de información no autorizadas.		

A.10.10.1	Registros de auditoría	*Control* Se deben elaborar registros de auditoría para las actividades de los usuarios, excepciones y eventos de seguridad de la información, y se deben mantener durante un período acordado para ayudar a futuras investigaciones y en la supervisión del control de acceso.
A.10.10.2	Supervisión del uso de sistemas	*Control* Se deben establecer procedimientos para hacer el seguimiento al uso de las instalaciones de procesamiento de la información, y se deben revisar regularmente los resultados de las actividades de seguimiento.
A.10.10.3	Protección de la información de registros (logs)	*Control* Los medios de registro y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.10.10.4	Registros del Administrador y el operador	*Control* Las actividades del operador y del administrador del sistema se deben registrar.
A.10.10.5	Registro de fallas	*Control* Las fallas se deben registrar, analizar y se deben tomar las acciones apropiadas.
A.10.10.6	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados con una fuente de horario confiable acordada.
A.11 CONTROL DE ACCESO		
A.11.1 Requisitos de negocio para el control del acceso *Objetivo:* controlar el acceso a la información.		
A.11.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos de acceso del negocio y de seguridad.
A.11.2 Gestión del acceso de usuarios *Objetivo:* asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.		
A.11.2.1	Registro de usuarios	*Control* Debe existir un procedimiento formal de registro y cancelación de registro para otorgar y revocar los accesos a todos los servicios y sistemas de información.
A.11.2.2	Gestión de privilegios	*Control* Se debe restringir y controlar la asignación y uso de privilegios.
A.11.2.3	Gestión de contraseñas del usuario	*Control* La asignación de contraseñas se debe controlar mediante un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	*Control* La dirección debe establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios.

A.11.3 Responsabilidades del usuario *Objetivo:* prevenir el acceso a usuarios no autorizados, y el robo o compromiso de la información y de las instalaciones de procesamiento de la información.		
A.11.3.1	Uso de contraseñas	*Control* Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y uso de las contraseñas.
A.11.3.2	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.3.3	Política de escritorio y pantalla limpios	*Control* Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.11.4 Control de acceso a redes *Objetivo:* prevenir el acceso no autorizado a servicios en red.		
A.11.4.1	Políticas sobre el uso de servicios en red	*Control* Los usuarios sólo deben tener acceso directo a los servicios para los que han sido autorizados específicamente.
A.11.4.2	Autenticación de usuarios para conexiones externas	*Control* Se deben usar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación de equipamiento en la red	*Control* La identificación automática del equipamiento debe ser considerada como medio de autenticar conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección de puertos de diagnóstico y configuración remotos	*Control* El acceso físico y lógico a los puertos de diagnóstico y configuración se debe controlar.
A.11.4.5	Separación en redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
A.11.4.6	Control de conexión de red	*Control* Para redes compartidas, especialmente las que se extienden a través de los límites de la organización, la capacidad de conexión de los usuarios a la red debe estar restringida, en línea con la política de control de acceso y los requisitos de las aplicaciones del negocio (véase el apartado 11.1).
A.11.4.7	Control de enrutamiento de red	*Control* Se deben implementar controles de enrutamiento para las redes, para asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.
A.11.5 Control de acceso al sistema operativo *Objetivo:* evitar el acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de conexión (log-on) seguros	*Control* El acceso a los sistemas operativos se debe controlar mediante un proceso de conexión (log-on) seguro

A.11.5.2	Identificación y autenticación de usuarios	*Control* Todos los usuarios deben tener un identificador único (ID del usuario) para su uso personal y exclusivo. Se debe escoger una técnica de autenticación adecuada para comprobar la identidad declarada de un usuario.
A.11.5.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.11.5.4	Uso de utilitarios (utilities) del sistema	*Control* El uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación se debe restringir y controlar estrictamente.
A.11.5.5	Desconexión automática de sesiones	*Control* Las sesiones inactivas se deben apagar después de un período de inactividad definido.
A.11.5.6	Limitación del tiempo de conexión	*Control* Se deben aplicar restricciones en los tiempos de conexión, para brindar seguridad adicional en aplicaciones de alto riesgo.
A.11.6 Control de acceso a la información y a las aplicaciones *Objetivo:* evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.		
A.11.6.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones del sistema de aplicaciones por parte de los usuarios se debe restringir de acuerdo con la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas sensibles	*Control* Los sistemas sensibles deben tener entornos informáticos dedicados (aislados).
A.11.7 Informática móvil y trabajo remoto *Objetivo:* garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y trabajo remoto.		
A.11.7.1	Informática y comunicaciones móviles	*Control* Se debe adoptar una política formal, y medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de recursos de informática y comunicaciones móviles.
A.11.7.2	Trabajo remoto	*Control* Se debe desarrollar e implementar una política, y procedimientos y planes operacionales para actividades de trabajo remoto.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
A.12.1 Requisitos de seguridad de los sistemas de información *Objetivo:* garantizar que la seguridad es parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de requisitos de seguridad	*Control* Las declaraciones de los requisitos del negocio para nuevos sistemas de información, o las mejoras a los existentes, deben especificar los requisitos para controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones *Objetivo:* evitar errores, pérdida, modificación no autorizada o mala utilización de la información en aplicaciones.		

A.12.2.1	Validación de los datos de entrada	*Control* Los datos de entrada a las aplicaciones se deben validar para asegurar que son correctos y apropiados.
A.12.2.2	Control de procesamiento interno	*Control* Se deben incorporar en las aplicaciones revisiones de validación para detectar cualquier corrupción de la información debida a errores de procesamiento o actos deliberados.
A.12.2.3	Integridad de los mensajes	*Control* Se deben identificar los requisitos para asegurar la autenticación y proteger la integridad de los mensajes en las aplicaciones, y se deben identificar e implementar controles apropiados.
A.12.2.4	Validación de los datos de salida	*Control* La salida de datos de una aplicación se debe validar para asegurar que el procesamiento de la información almacenada es correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos *Objetivo:* proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión de llaves	*Control* Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.
A.12.4 Seguridad de los archivos del sistema *Objetivo:* garantizar la seguridad de los archivos del sistema.		
A.12.4.1	Control del software en producción	*Control* Se deben implementar procedimientos para controlar la instalación del software sobre sistemas en producción.
A.12.4.2	Protección de los datos de prueba del sistema	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.12.4.3	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte *Objetivo:* mantener la seguridad del software y la información del sistema de aplicaciones.		
A.12.5.1	Procedimientos de control de cambios	*Control* La implementación de los cambios se debe controlar estrictamente mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	*Control* Cuando los sistemas operativos cambian, las aplicaciones críticas del negocio se deben revisar y poner a prueba para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.

A.12.5.3	Restricciones en los cambios a los paquetes de software	*Control* Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.12.5.4	Fuga de información	*Control* Se deben impedir las oportunidades para fuga de información.
A.12.5.5	Desarrollo externo de software	*Control* El desarrollo de software contratado externamente debe ser supervisado y la organización debe hacer seguimiento de esto.
A.12.6 Gestión de la vulnerabilidad técnica *Objetivo:* reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	*Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debe evaluar la exposición de la organización a estas vulnerabilidades, y se deben tomar las medidas apropiadas tomadas para abordar el riesgo asociado.
A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A.13.1 Reporte de eventos y debilidades de seguridad de la información *Objetivo:* asegurar que los eventos y debilidades de seguridad de la información asociados con los sistemas de información se comunican de una manera que permite que se tomen acciones correctivas oportunas.		
A.13.1.1	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben reportar a través de los canales de gestión apropiados, lo más rápidamente posible.
A.13.1.2	Reporte de las debilidades de seguridad	*Control* Todos los empleados, contratistas y usuarios por tercera parte, de sistemas y servicios de información, deben observar y reportar cualquier debilidad en la seguridad de sistemas o servicios, observada o que se sospeche.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información *Objetivo:* asegurar que se aplica un método consistente y eficaz a la gestión de los incidentes de seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	*Control* Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.
A.13.2.2	Aprendiendo de los incidentes de seguridad de la información	*Control* Se deben implementar mecanismos para posibilitar que los tipos, volúmenes y costos de los incidentes de seguridad de la información sean cuantificados y se les haga seguimiento.
A.13.2.3	Recolección de evidencia	*Control* En donde una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información involucra acciones legales (ya sea civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para evidencia establecidas en la jurisdicción pertinente.

A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio *Objetivo:* contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas o desastres de gran magnitud en los sistemas de información, y asegurar su reanudación oportuna.		
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	*Control* Se debe desarrollar y mantener un proceso gestionado para la continuidad del negocio en toda la organización, que aborde los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación de riesgos	*Control* Se deben identificar los eventos que pueden causar interrupciones en los procesos del negocio, junto con la probabilidad e impacto de estas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	*Control* Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla de los procesos críticos del negocio.
A.14.1.4	Estructura para la planificación de la continuidad del negocio	*Control* Se debe mantener una sola estructura de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, abordar en forma consistente los requisitos de seguridad de la información, e identificar prioridades para ensayo y mantenimiento.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	*Control* Los planes de continuidad del negocio se deben poner a prueba y actualizar regularmente para asegurar que estén actualizados y sean eficaces.
A.15 CUMPLIMIENTO		
A.15.1 Cumplimiento de los requisitos legales *Objetivo:* evitar incumplimiento de cualquier ley, obligación estatutaria, reglamentaria o contractual, y de cualquier requisito de seguridad.		
A.15.1.1	Identificación de la legislación aplicable	*Control* Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.
A.15.1.2	Derechos de propiedad intelectual (DPI)	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales sobre el uso de material con respecto al cual puede haber derechos de propiedad intelectual, y sobre el uso de productos de software patentados.
A.15.1.3	Protección de los registros de la organización	*Control* Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

A.15.1.4	Protección de los datos y privacidad de la información personal	*Control* Se debe asegurar la protección y privacidad de los datos, como se exige en la legislación, reglamentaciones, y si es aplicable, cláusulas contractuales pertinentes.
A.15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información	*Control* Se debe impedir que los usuarios usen las instalaciones de procesamiento de la información para propósitos no autorizados.
A.15.1.6	Regulación de los controles criptográficos	*Control* Deben utilizarse controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones relevantes.
A.15.2 Cumplimiento de políticas y normas de seguridad y cumplimiento técnico *Objetivo:* asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.		
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	*Control* Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de las políticas y normas de seguridad.
A.15.2.2	Verificación del cumplimiento técnico	*Control* Se debe verificar regularmente el cumplimiento de las normas de implementación de seguridad.
A.15.3 Consideraciones de la auditoría de sistemas de información *Objetivo:* maximizar la eficacia del proceso de auditoría de sistemas de información y minimizar la interferencia desde y hacia éste.		
A.15.3.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que involucran verificaciones sobre sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información	*Control* Se debe proteger el acceso a las herramientas de auditoría del sistema de información, para evitar que se pongan en peligro o que se haga un uso inadecuado de ellas.

ANEXO B
(Informativo)

PRINCIPIOS DE LA OCDE Y DE ESTA NORMA CUBANA

Los principios presentados en la Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información se aplican a todos los niveles de política y operacionales que controlan la seguridad de los sistemas y redes de información. Esta Norma Cubana brinda una estructura del sistema de gestión de la seguridad de la información para implementar algunos principios de la OCDE usando el modelo PHVA y los procesos descritos en los apartados 4, 5, 6 y 8, como se indica en la Tabla B.1.

Tabla B.1. Principios de la OCDE y el modelo PHVA

Principio OCDE	Proceso de SGSI correspondiente y fase de PHVA
Toma de conciencia Los participantes deben estar conscientes de la necesidad de seguridad de los sistemas y redes de información y de lo que pueden hacer para mejorar la seguridad.	Esta actividad es parte de la fase *Hacer* (véanse los apartados 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables por la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase *Hacer* (véanse los apartados 4.2.2 y 5.1)
Respuesta Los participantes deberían actuar de una manera oportuna y en cooperación para evitar, detectar y responder ante incidentes de seguridad.	Ésta es en parte una actividad de seguimiento de la fase *Verificar* (véanse los apartados 4.2.3 y 6 a 7.3 y una actividad de respuesta de la fase *Actuar* (véanse los apartados 4.2.4 y 8.1 a 8.3). Esto también se puede cubrir por algunos aspectos de las fases *Planificar* y *Verificar*.
Evaluación de riesgos Los participantes deberían realizar evaluaciones de los riesgos.	Esta actividad es parte de la fase *Planificar* (véase el apartado 4.2.1) y la revaloración del riesgo es parte de la fase *Verificar* (véanse los apartados 4.2.3 y 6 a 7.3).
Diseño e implementación de la seguridad Los participantes deberían incorporar la seguridad como un elemento esencial de los sistemas y redes de información.	Una vez que se ha realizado la valoración de riesgos, se seleccionan controles para el tratamiento de riesgos como parte de la fase *Planificar* (véase el apartado 4.2.1). La fase *Hacer* (véanse los apartados 4.2.2 y 5.2) cubre la implementación y el uso operacional de estos controles.
Gestión de la seguridad Los participantes deberían adoptar un enfoque amplio hacia la gestión de la seguridad.	La gestión de riesgos es un proceso que incluye la prevención, detección y respuesta a incidentes, mantenimiento, auditorías y revisión continuos. Todos estos aspectos están cobijados en las fases de *Planificar, Hacer, Verificar y Actuar*.
Revaloración Los participantes deberían revisar y revalorar la seguridad de los sistemas y redes de información, y hacer las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos de seguridad.	La revaloración de la seguridad de la información es una parte de la fase *Verificar* (véanse los apartados 4.2.3 y 6 a 7.3), en donde se deberían realizar revisiones regulares para verificar la eficacia del sistema de gestión de la seguridad de la información; y la mejora de la seguridad es parte de la fase *Actuar* (véanse los apartados 4.2.4 y 8.1 a 8.3).

ANEXO C
(Informativo)

CORRESPONDENCIA ENTRE LA NORMA ISO 9001:2000, LA NORMA ISO 14001:2004, Y LA PRESENTE NORMA CUBANA

La Tabla C.1 muestra la correspondencia entre la norma ISO 9001:2000, la norma ISO 14001:2004 y la presente Norma Cubana

Tabla C.1. Correspondencia entre la ISO 9001:2000, la ISO 14001:2004 y la presente norma internacional

Esta norma internacional	ISO 9001:2000	ISO 14001:2004
0. Introducción 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Compatibilidad con otros sistemas de gestión	**0. Introducción** 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Relación con la norma ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	**Introducción**
1. Objeto 1.1 Generalidades 1.2 Aplicación	**1. Objeto y campo de aplicación** 1.1 Generalidades 1.2 Aplicación	**1. Objeto y campo de aplicación**
2 Referencias normativas	**2. Referencias normativas**	**2. Normas para consulta**
3 Términos y definiciones	**3 Términos y definiciones**	**3. Términos y definiciones**
4. Sistema de gestión de la seguridad de la información 4.1 Requisitos generales 4.2 Establecimiento y gestión del SGSI 4.2.1 Establecimiento del SGSI 4.2.2 Implementación y operación del SGSI 4.2.3 Seguimiento y revisión del SGSI 4.2.4 Mantenimiento y mejora del SGSI 4.3 Requisitos de documentación 4.3.1 Generalidades 4.3.2 Control de documentos 4.3.3 Control de registros	**4. Sistema de gestión de la calidad** 4.1 Requisitos generales 8.2.3 Seguimiento y medición de los procesos 8.2.4 Seguimiento y medición del Producto 4.2 Requisitos de documentación 4.2.1 Generalidades 4.2.2 Manual de calidad 4.2.3 Control de documentos 4.2.4 Control de registros	**4. Requisitos del sistema de gestión ambiental** 4.1 Requisitos generales 4.4 Implementación y operación 4.5.1 Seguimiento y medición 4.4.5 Control de documentos 4.5.4 Control de registros
5. Responsabilidad de la dirección 5.1 Compromiso de la dirección	**5. Responsabilidad de la dirección** 5.1 Compromiso de la dirección 5.2 Enfoque al cliente 5.3 Política de calidad 5.4 Planificación 5.5 Responsabilidad, autoridad y comunicación	 4.2 Política ambiental 4.3 Planificación
5.2 Gestión de recursos 5.2.1 Provisión de recursos 5.2.2 Formación, toma de conciencia y competencia	**6. Gestión de los recursos** 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Competencia, toma de conciencia y formación 6.3 Infraestructura 6.4 Ambiente de trabajo	 4.2.2 Competencia, formación y toma de conciencia

6. Auditorías internas del SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7. Revisión del SGSI por la dirección 7.1 Generalidades 7.2 Información para la revisión 7.3 Resultados de la revisión	**5.6 Revisión por la dirección** 5.6.1 Generalidades 5.6.2 Información para la revisión 5.6.3 Resultados de la revisión	**4.6 Revisión por la dirección**
8. Mejora del SGSI 8.1 Mejora continua	**8.5 Mejora** 8.5.2 Mejora continua	
8.2 Acción correctiva	8.5.3 Acciones correctivas	4.5.3 No conformidad, acción correctiva y acción preventiva
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles Anexo B Principios de la OCDE y esta norma Anexo C Correspondencia entre la ISO 9001:2000, la ISO 14001:2004 y esta Norma Internacional	Anexo A Correspondencia entre la ISO 9001:2000 y la ISO 14001:1996	Anexo A Orientación para el uso de esta norma internacional Anexo B Correspondencia entre la ISO 14001 y la ISO 9001

BIBLIOGRAFÍA

[1] ISO 9001:2000, *Quality Management Systems. Requirements.*

[2] ISO/IEC 13335-1:2004, *Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management*

[3] ISO/IEC TR 13335-3:1998, *Information Technology - Guidelines for the Management of IT Security. Part 3: Techniques for the Management of IT Security.*

[4] ISO/IEC TR 13335-4:2000, *Information Technology - Guidelines for the Management of IT Security. Part 4: Selection of Safeguards.*

[5] ISO 14001:2204, *Environmental Management Systems - Requirements with Guidance for use.*

[6] ISO/IEC TR 18044:2004, *Information Technology - Security Techniques. Information Security Incident Management.*

[7] ISO 19011:2002, *Guidelines for Quality and/or Environmental Management Systems Auditing.*

[8] ISO/IEC Guide 62:1996, *General Requirements for Bodies Operating Assessment and Certification/registration of Quality Systems.*

[9] ISO/IEC Guide 73:2002, *Risk Management – Vocabulary - Guidelines for use in Standards.*

Otras publicaciones

[1] OECD, *Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, Paris: OECD, July 2002. www.oecd.org.*

[2] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

[3] Deming W.E., *Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986.*