ESTÁNDAR INTERNACIONAL

ISO/IEC 27001

Primera Edicion
2005 - 10 - 15

Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Numero de Referencia
ISO/IEC 27001:2005 (E)

SOLO PARA FINES DIDACTICOS

Tabla de Contenido

SOLO PARA FINES DIDACTICOS

SOLO PARA FINES DIDACTICOS

Prefacio

ISO (la Organización Internacional para la Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización universal. Los organismos nacionales miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de comités técnicos establecidos por la organización respectiva para lidiar con campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no-gubernamentales, junto con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido u comité técnico conjunto, ISO/IEC JTC 1.

Los Estándares Internacionales son desarrollados en concordancia con las reglas dadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico conjunto con enviados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

Se debe prestar atención a la posibilidad que algunos elementos de este documento estén sujetos a derechos de patente. ISO e IEC no deben ser responsables de la identificación de algún o todos los derechos de patentes.

ISO/IEC 27001 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

SOLO PARA FINES DIDACTICOS

0 Introducción

0.1 General

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

0.2 Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) monitorear y revisar el desempeño y la efectividad del SGSI; y
d) mejoramiento continúo en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Figura 1 muestra cómo un SGSI

SOLO PARA FINES DIDACTICOS

toma como Insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. La Figura 1 también muestra los vínculos en los procesos presentados en las Cláusulas 4, 5, 6, 7 y 8.

La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD (2002)[1] que gobiernan los sistemas y redes de seguridad de la información. Este Estándar Internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

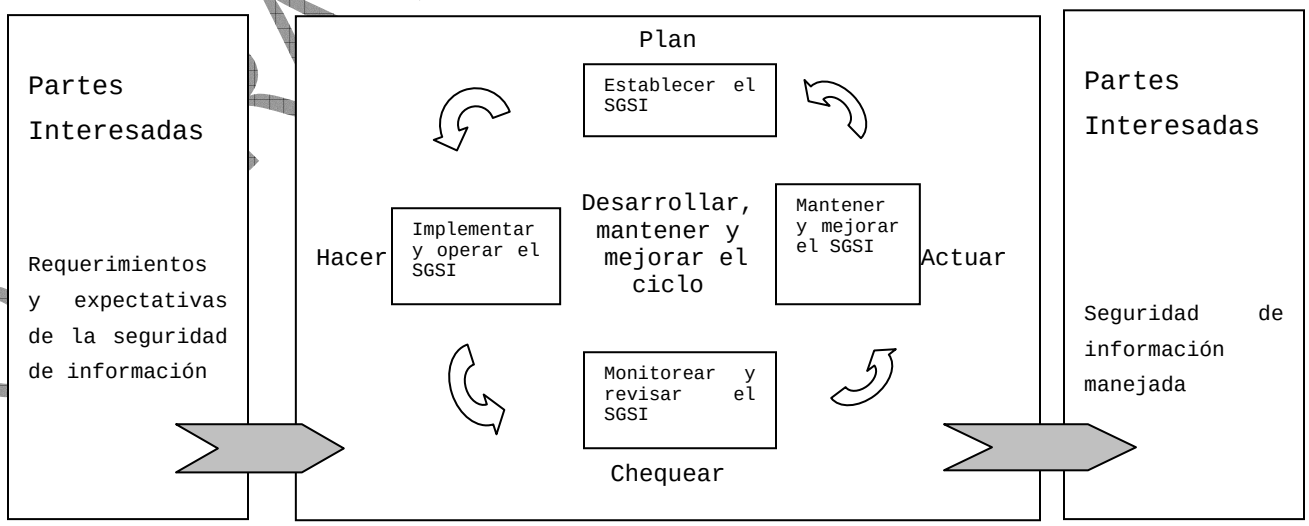
EJEMPLO 1

Un requerimiento podría ser que las violaciones de seguridad de la información no causen daño financiero a la organización y/o causen vergüenza a la organización.

EJEMPLO 2

Una expectativa podría ser que si ocurre un incidente serio –tal vez el pirateo del web site eBusiness de una organización- debería contarse con las personas con la capacitación suficiente en los procedimientos apropiados para minimizar el impacto.

Figura 1 – Modelo PDCA aplicado a los procesos SGSI



[1] Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. Paris: OECD, Julio 2002. www.oecd.org.

SOLO PARA FINES DIDACTICOS

Planear (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

0.3 Compatibilidad con otros sistemas de gestión

Este Estándar Internacional se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares. La Tabla C.1 muestra la relación entre las cláusulas de este Estándar Internacional, ISO 9001:2000 e ISO 14001:2004.

Este Estándar Internacional está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado.

SOLO PARA FINES DIDACTICOS

Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Importante – No es el propósito de esta publicación incluir todas las provisiones necesarias de un contrato. Los usuarios son responsables de su correcta aplicación. El cumplimiento de un Estándar Internacional no quiere decir que confiere inmunidad de las obligaciones legales **.**

1 Alcance

1.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

NOTA 1: Las referencias a 'comerciales' en este Estándar Internacional se deben implementar ampliamente para significar aquellas actividades que son básicas para los propósitos de la existencia de la organización.

NOTA 2: ISO/IEC 17799 proporciona un lineamiento de implementación que se puede utilizar cuando se diseñan controles.

1.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

SOLO PARA FINES DIDACTICOS

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

NOTA: Si una organización ya cuenta con un sistema de gestión de procesos comerciales operativos (por ejemplo, en relación con ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requerimientos de este Estándar Internacional dentro de este sistema de gestión existente.

2 Referencias normativas

Los siguientes documentos mencionados son indispensables para la aplicación de este documento. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento citado.

ISO/IEC 17799:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

3 Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

3.1
activo

cualquier cosa que tenga valor para la organización
(ISO/IEC 13335-1:2004)

3.2
disponibilidad

la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada
(ISO/IEC 13335-1:2004)

SOLO PARA FINES DIDACTICOS

3.3

confidencialidad

la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

(ISO/IEC 13335-1:2004)

3.4

seguridad de información

preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad

(ISO/IEC 17799:2005)

3.5

evento de seguridad de la información

una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

(ISO/IEC TR 18044:2004)

3.6

incidente de seguridad de la información

un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

(ISO/IEC TR 18044:2004)

3.7

sistema de gestión de seguridad de la información SGSI

esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

NOTA: El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos

3.8

integridad

la propiedad de salvaguardar la exactitud e integridad de los activos.

(ISO/IEC 13335-1:2004)

SOLO PARA FINES DIDACTICOS

3.9

riesgo residual

el riesgo remanente después del tratamiento del riesgo

(ISO/IEC Guía 73:2002)

3.10

aceptación de riesgo

decisión de aceptar el riesgo

(ISO/IEC Guía 73:2002)

3.11

análisis de riesgo

uso sistemático de la información para identificar fuentes y para estimar el riesgo

(ISO/IEC Guía 73:2002)

3.12

valuación del riesgo

proceso general de análisis del riesgo y evaluación del riesgo

(ISO/IEC Guía 73:2002)

3.13

evaluación del riesgo

proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo

(ISO/IEC Guía 73:2002)

3.14

gestión del riesgo

actividades coordinadas para dirigir y controlar una organización con relación al riesgo

(ISO/IEC Guía 73:2002)

3.15

tratamiento del riesgo

proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo

(ISO/IEC Guía 73:2002)

NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

3.16

enunciado de aplicabilidad

SOLO PARA FINES DIDACTICOS

enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

NOTA: Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la organización para la seguridad de la información.

4 Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA que se muestra en la Figura 1.

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

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

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

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

   2) tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;

   3) esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;

   4) establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);

   5) haya sido aprobada por la gerencia.

SOLO PARA FINES DIDACTICOS

NOTA: Para propósitos de este Estándar Internacional, la política SGSI es considerada como un super-conjunto de la política de seguridad de la información. Estas políticas se pueden describir en un documento.

c) Definir el enfoque de valuación del riesgo de la organización

1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.

2) Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

NOTA: Existen diferentes metodologías para el cálculo del riesgo. Los ejemplos de las metodologías de cálculo del riesgo se discuten en ISO/IEC TR 13335-3, Tecnología de información – Lineamiento para la gestión de la Seguridad TI – Técnicas para la gestión de la Seguridad TI

d) Identificar los riesgos

1) Identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos.

2) Identificar las amenazas para aquellos activos.

3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.

4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analizar y evaluar el riesgo

1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.

3) Calcular los niveles de riesgo.

---

[2] El término ‘propietario’ identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término ‘propietario’ no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

SOLO PARA FINES DIDACTICOS

4) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).

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

Las acciones posibles incluyen:

1) aplicar los controles apropiados;
2) aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo (ver 4.2.1 c)2)) de la organización;
3) evitar los riesgos; y
4) transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores.

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

Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver 4.2.1(c), así como los requerimientos legales, reguladores y contractuales.

Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.

NOTA: El Anexo A contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones. Se dirige a los usuarios de este Estándar Internacional como un punto de inicio para la selección de controles para asegurar que no se pase por alto ninguna opción de control importante.

h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

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

j) Preparar un Enunciado de Aplicabilidad

Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1 (g) y las razones para su selección

2) los objetivos de control y controles implementados actualmente (ver 4.2.1 (e) 2); y

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

NOTA: El Enunciado de Aplicabilidad proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo. El justificar las exclusiones proporciona un chequeo para asegurar que ningún control haya sido omitido inadvertidamente.

SOLO PARA FINES DIDACTICOS

4.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información (ver 5).

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1(g) para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3 c)).

NOTA: La medición de la efectividad de los controles permite a los gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

e) Implementar los programas de capacitación y conocimiento (ver 5.2.2).

f) Manejar las operaciones del SGSI.

g) Manejar recursos para el SGSI (ver 5.2).

h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad.

4.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:

   1) detectar prontamente los errores en los resultados de procesamiento;

   2) identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos;

   3) permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;

   4) ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y

   5) determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorias de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

SOLO PARA FINES DIDACTICOS

c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:

   1) la organización;
   2) tecnología;
   3) objetivos y procesos comerciales;
   4) amenazas identificadas;
   5) efectividad de los controles implementados; y
   6) eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

e) Realizar auditorias SGSI internas a intervalos planeados (ver 6).

NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI (ver 7.1).

g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI (ver 4.3.3).

4.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

b) Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

SOLO PARA FINES DIDACTICOS

4.3 Requerimientos de documentación

4.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles.

Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI.

La documentación SGSI debe incluir lo siguiente:

a) enunciados documentados de la política SGSI (ver 4.2.1b)) y los objetivos;
b) el alcance del SGSI (ver 4.2.1a));
c) procedimientos y controles de soporte del SGSI;
d) una descripción de la metodología de evaluación del riesgo (ver 4.2.1c));
e) reporte de evaluación del riesgo (ver 4.2.1c) a 4.2.1g));
f) plan de tratamiento del riesgo (ver 4.2.2b));
g) Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c));
h) registros requeridos por este Estándar Internacional (ver 4.3.3); y
i) Enunciado de Aplicabilidad.

NOTA 1: Cuando aparece el término 'procedimiento documentado' dentro este Estándar Internacional, significa que el procedimiento se establece, documenta, implementa y mantiene.

NOTA 2: La extensión de la documentación SGSI puede diferir de una organización a otro debido a:

- el tamaño de la organización y el tipo de sus actividades; y
- el alcance y complejidad de los requerimientos de seguridad y el sistema que se está manejando.

NOTA 3: Los documentos y registros pueden estar en cualquier forma o medio.

4.3.2 Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones gerenciales necesarias para:

a) aprobar la idoneidad de los documentos antes de su emisión;
b) revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos;
c) asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos;

SOLO PARA FINES DIDACTICOS

d) asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
e) asegurar que los documentos se mantengan legibles y fácilmente identificables;
f) asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;
g) asegurar que se identifiquen los documentos de origen externo;
h) asegurar que se controle la distribución de documentos;
i) evitar el uso indebido de documentos obsoletos; y
j) aplicarles una identificación adecuada si se van a retener por algún propósito.

4.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.

EJEMPLO
Son ejemplos de registros los libros de visitantes, los registros de auditoria y las solicitudes de autorización de acceso.

5 Responsabilidad de la gerencia

5.1 Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

a) establecer una política SGSI;
b) asegurar que se establezcan objetivos y planes SGSI;
c) establecer roles y responsabilidades para la seguridad de información;
d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;

SOLO PARA FINES DIDACTICOS

e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1);
f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
g) asegurar que se realicen las auditorías internas SGSI (ver 6); y
h) realizar revisiones gerenciales del SGSI (ver 7).

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

a) establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;
b) asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
c) identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
d) mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
e) llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
f) donde se requiera, mejorar la efectividad del SGSI.

5.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para:

a) determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
b) proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades;
c) evaluar la efectividad de las acciones tomadas;
d) mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (ver 4.3.3).

La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

SOLO PARA FINES DIDACTICOS

6 Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

a) cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes;
b) cumplen con los requerimientos de seguridad de la información identificados;
c) se implementan y mantienen de manera efectiva; y
d) se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de 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.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros (ver 4.3.3) se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación (ver 8).

NOTA: ISO 19011:2002, Lineamiento para auditar sistemas de gestión de calidad y/o ambiental, puede proporcionar un lineamiento útil para llevar a cabo auditorías internas.

7 Revisión Gerencial del SGSI

7.1 General

La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros (ver 4.3.3).

SOLO PARA FINES DIDACTICOS

7.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

a) resultados de auditorias y revisiones del SGSI;
b) retroalimentación de las partes interesadas;
c) técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
d) status de acciones preventivas y correctivas;
e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
f) resultados de mediciones de efectividad;
g) acciones de seguimiento de las revisiones gerenciales previas;
h) cualquier cambio que pudiera afectar el SGSI; y
i) recomendaciones para el mejoramiento.

7.3 Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente:

a) mejoramiento de la efectividad del SGSI;
b) actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
c) modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    1) requerimientos comerciales;
    2) requerimientos de seguridad;
    3) procesos comerciales que afectan los requerimientos comerciales existentes;
    4) requerimientos reguladores o legales;
    5) obligaciones contractuales; y
    6) niveles de riesgo y/o criterio de aceptación del riesgo.
d) necesidades de recursos;
e) mejoramiento de cómo se mide la efectividad de los controles.

SOLO PARA FINES DIDACTICOS

8 Mejoramiento del SGSI

8.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

a) identificar las no-conformidades;
b) determinar las causas de las no-conformidades;
c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
d) determinar e implementar la acción correctiva necesaria;
e) registrar los resultados de la acción tomada (ver 4.3.3); y
f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

a) identificar las no-conformidades potenciales y sus causas;
b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
c) determinar e implementar la acción preventiva necesaria;
d) registrar los resultados de la acción tomada (ver 4.3.3); y
e) revisar la acción preventiva tomada.

La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo.

SOLO PARA FINES DIDACTICOS

NOTA La acción para evitar las no-conformidades con frecuencia es más una acción efectiva en costo que la acción correctiva.

SOLO PARA FINES DIDACTICOS

Anexo A

(Normativo)

Objetivos de control y controles

Los objetivos de control y los controles enumerados en la Tabla A.1 se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en 4.2.1.

El BS ISO/IEC 17799:2005 Cláusulas del 5 al 15 proporciona consulta y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en A.5 al A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad
A.5.1 Política de seguridad de información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad

de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A,6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A.6.2 Entidades externas		

SOLO PARA FINES DIDACTICOS

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
A.7 Gestión de activos		
A.7.1 *Responsabilidad por los activos*		
Objetivo*:* Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; 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 los activos asociados con los medios de procesamiento de la información deben ser 'propiedad'[3] de una parte designada de a organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información		
Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

[3] Explicación: El término 'propietario' identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

SOLO PARA FINES DIDACTICOS

A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo[4] Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 *Durante el empleo* Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las

[4] Explicación: Aquí la palabra 'empleo' se utiliza para abarcar todas las siguientes situaciones diferentes: empleo de personas (temporal o larga duración), asignación de roles laborales, cambios de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

SOLO PARA FINES DIDACTICOS

		responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad física y ambiental		
A.7.1 *Áreas seguras* Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 *Seguridad del equipo* Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

SOLO PARA FINES DIDACTICOS

A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

SOLO PARA FINES DIDACTICOS

A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 *Protección contra software malicioso y código móvil* Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	*Back-up o respaldo de la información*	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 *Gestión de seguridad de redes* 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 ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios		

SOLO PARA FINES DIDACTICOS

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información	Control

SOLO PARA FINES DIDACTICOS

	disponible públicamente	Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoria*	Control Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		

SOLO PARA FINES DIDACTICOS

A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la

SOLO PARA FINES DIDACTICOS

		identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de

SOLO PARA FINES DIDACTICOS

		procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de 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 clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en 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 de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar 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 se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la

SOLO PARA FINES DIDACTICOS

		organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los

SOLO PARA FINES DIDACTICOS

	continuidad comercial	requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

SOLO PARA FINES DIDACTICOS

A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	*Cumplimiento con las políticas y estándares de seguridad*	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	*Chequeo de cumplimiento técnico*	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoria de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoria de los sistema de información.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Anexo B

(Informativo)

Principios OECD y este Estándar Internacional

Los principios dados en los Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información [1] se aplican a toda las políticas y niveles operacionales que gobiernan la seguridad de los sistemas y redes de información. Este Estándar Británico proporciona un marco referencial del sistema de gestión de la seguridad de la información para implementar algunos de los principios OECD utilizando el modelo PDCA y los procesos descritos en las Cláusulas 4, 5, 6 y 8 como se indica en la Tabla B.1.

Tabla B.1 – Principios OECD y el modelo PDCA

Principio OECD	Proceso SGSI correspondiente y fase PDCA
Conciencia	Esta actividad es parta de la fase **Hacer**

SOLO PARA FINES DIDACTICOS

Los participantes deben estar al tanto de la necesidad de seguridad de los sistemas y redes de información y lo que pueden hacer para aumentar la seguridad	(ver 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables de la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase **Hacer** (ver 4.2.2 y 5.1)
Respuesta Los participantes deben actuar de manera oportuna y cooperativa para evitar, detectar y responder a los incidentes de seguridad.	Esta es en parte una actividad de monitoreo de la fase **Chequear** (ver 4.2.3 y 6 al 7.3) y una actividad de respuesta de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3). Esto también puede ser abarcado por algunos aspectos de las fases **Planear** y **Chequear**.
Evaluación del riesgo Los participantes deben realizar evaluaciones de riesgo.	Esta actividad es una parte de la fase **Planear** (ver 4.2.1) y la evaluación del riesgo es parte de la fase **Chequear** (ver 4.2.3 y 6 al 7.3).
Diseño e implementación de la seguridad Los participantes deben incorporar la seguridad como un elementos esencial de los sistemas y redes de información.	Una vez que se ha completado la evaluación del riesgo, se seleccionan los controles para el tratamiento de riesgos como una parte de la fase **Planear** (ver 4.2.1). La fase **Hacer** (ver 4.2.2 y 5.2) entonces abarca la implementación y uso operacional de estos controles.
Gestión de la seguridad Los participantes deben adoptar un enfoque integral para la gestión de la seguridad.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta a los incidentes, mantenimiento continuo, revisión y auditoria. Todos estos aspectos son parte de las fases **Planear, Hacer, Chequear y Actuar.**
Reevaluación Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información, y realizar las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos.	La reevaluación de la seguridad de la información es una parte de la fase **Chequear** (ver 4.2.3 y 6 a 7.3) donde se deben realizar revisiones regulares para chequear la efectividad del sistema de gestión de seguridad de la información, y mejorar la seguridad es parte de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3).

SOLO PARA FINES DIDÁCTICOS

SOLO PARA FINES DIDACTICOS

Anexo C

(Informativo)

Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

La tabla C.1 muestra la correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

Tabla C.1 – Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

Este Estándar Internacional	ISO 9001:2000	ISO 14001:2004
Introducción General Enfoque del proceso Compatibilidad con otros sistemas de gestión	**0 Introducción** 0.1 General 0.2 Enfoque del proceso 0.3 Relación con ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	**Introducción**
1 Alcance 1.1 General 1.2 Aplicación	**1 Alcance** 1.1 General 1.2 Aplicación	**1 Alcance**
2 Referencias normativas	**2 Referencia normativa**	**2 Referencia normativa**
3 Términos y definiciones	**3 Términos y definiciones**	**3 Términos y definiciones**
4 Sistema de gestión de la seguridad de la información 4.1 Requerimientos generales 4.2 Establecer y manejar el SGSI 4.2.1 Establecer el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Monitorear y revisar el SGSI 4.2.4 Mantener y mejorar el SGSI 4.3 Requerimientos de documentación 4.3.1 General 4.3.2 Control de documentos 4.3.3 Control de registros	**4 Sistema de gestión de calidad** 4.1 Requerimientos generales 8.2.3 Monitoreo y medición de procesos 8.2.4 Monitoreo y medición del producto 4.2 Requerimientos de documentación 4.2.1 General 4.2.2 Manual de calidad 4.2.3 Control de documentos 4.2.4 Control de registros	**4 Requerimientos EMS** 4.1 Requerimientos generales 4.4 Implementación y operación 4.5.1 Monitoreo y medición ´ 4.4.5 Control de documentación 4.5.4 Control de registros
5 Responsabilidad de gestión 5.1 Compromiso de la gerencia	**5 Responsabilidad de gestión** 5.1 Compromiso de la gerencia 5.2 Enfoque del cliente 5.3 Política de calidad 5.4 Planeación 5.5 Responsabilidad, autoridad y comunicación	 4.2 Política ambiental 4.3 Planeación
5.2 Manejo de recursos 5.2.1 Provisión de recursos 5.2.2 Capacitación, conciencia y capacidad	**6 Manejo de recursos** 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Capacidad, conciencia y capacitación 6.3 Infraestructura 6.4 Ambiente laboral	 4.4.2 Competencia, capacitación y conciencia
6 Auditorías internas SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna

SOLO PARA FINES DIDACTICOS

7 Revisión gerencial del SGSI 7.1 General 7.2 Insumo de la revisión 7.3 Output de la revisión	**5.6 Revisión gerencial** 5.6.1 General 5.6.2 Insumo de la revisión 5.6.3 Output de la revisión	**4.6 Revisión gerencial**
8 Mejoramiento SGSI 8.1 Mejoramiento continuo 8.2 Acción correctiva 8.3 Acción preventiva	**8.5 Mejoramiento** 8.5.2 Mejoramiento continuo 8.5.3 Acciones correctivas 8.5.3 Acciones preventivas	 4.5.3 No-conformidad y acción correctiva y preventiva
Anexo A Objetivos de control y controles **Anexo B Principios OECD y este Estándar Internacional** **Anexo C Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional**	 **Anexo A Correspondencia entre ISO 9001:2000 e ISO 14001:1996**	**Anexo A Lineamiento sobre el uso de este Estándar Internacional** **Anexo B Correspondencia entre ISO 14001:2004 e ISO 9001_2000**

Bibliografía

Publicación de estándares

(1) ISO 9001:2000, Sistemas de gestión de calidad - Requerimientos

(2) ISO/IEC 13335-1:204, Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones

(3) ISO/IEC TR 13335-3:1998, *Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI*

(4) ISO/IEC 13335-4:2000, *Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas*

(5) ISO 14001:2004, Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso

(6) ISO/IEC TR 18044:2004, Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información

(7) ISO/IEC 19011:2002, Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental

(8) ISO/IEC Guía 62:1996, *Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.*

(9) ISO/IEC Guía 73:2002, Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares

Otras publicaciones

(1) OECD, *Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información – Hacia una Cultura de Seguridad*. Paris: OECD, Julio 2002, www.oecd.org

(2) NIST SP 800-30, Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información

(3) Deming, W.E., Fuera de la Crisis, Cambridge, Mass:MIT, Centro de Estudios de Ingeniería Avanzada, 1986

SOLO PARA FINES DIDACTICOS