NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27001
2008

Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias - INDECOPI
Calle De La Prosa 138, San Borja (Lima 41) Apartado 145 Lima, Perú

EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

EDI. Information technology. Security techniques. Information security management systems. Requirements

(EQV. ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements)

2008-12-12
1ª Edición

R.0042-2008/INDECOPI-CNB. Publicada el 2009-01-11 Precio basado en 49 páginas
I.C.S: 35.040 ESTA NORMA ES RECOMENDABLE
Descriptores: Administración de seguridad de la información, información.

ÍNDICE

PREFACIO

A. RESEÑA HISTÓRICA

A.1 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos (EDI), mediante el Sistema 1 o Adopción, durante los meses de mayo a octubre del 2008, utilizando como antecedente la ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

A.2 El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos – EDI presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias -CNB-, con fecha 2008-10-22, el PNTP-ISO/IEC 27001:2008, para su revisión y aprobación, siendo sometido a la etapa de Discusión Pública el 2008-11-13. No habiéndose presentado observaciones fue oficializado como Norma Técnica Peruana **PNTP-ISO/IEC 27001:2008 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos**, 1ª Edición, el 11 de enero de 2009.

A.3 Esta Norma Técnica Peruana reemplaza a la NTP 821.101:2005 EDI. Sistemas de gestión de seguridad de la información. Especificaciones con guía de uso y es una adopción de la ISO/IEC 27001:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

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

Secretaría	EAN PERU
Presidente	Marcos Suárez
Secretaria	Mary Wong

ENTIDAD	REPRESENTANTE
DISTRIBUIDORA MAYORISTA SYMBOL S.A.	Deyanira Villanueva Walter Equizabel
DROKASA PERU S.A.	Juan Cruz Valdez
E. WONG S.A.	Marcela Aparicio Rolando Bartra
FOLIUM S.A.C.	Roberto Huby
IBC SOLUTIONS PERU S.A.C.	Oscar Velasquez Daniella Orellana
ITS CONSULTANTS S.A.C.	Ricardo Dioses
OFICINA DE NORMALIZACION PREVISIONAL	Roberto Puyó
PONT. UNIV. CATOLICA DEL PERU	Viktor Khlebnikov Willy Carrera
PRESIDENCIA DEL CONSEJO DE MINISTROS	Max Lazaro Cesar Vilchez
PROCTER & GAMBLE DEL PERU S.A.	Javier Kameya
SUPERINTENDENCIA DE ADMINISTRACION TRIBUTARIA - SUNAT	Daniel Llanos
TECNOLOGÍA FLEXOGRAFICA S.A.	Luis Chávez Saavedra
TCI S.A.	Renzo Alcántara
UNILEVER ANDINA PERU S.A.	Rolando Rivadeneira
GS1 PERU	Milagros Dávila Tatiana Peña

INTRODUCCIÓN

0.1 Aspectos generales

Esta Norma Técnica Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de la Información ISMS, por sus siglas en Inglés (Information Security Management System). La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como que las situaciones simples requieran soluciones ISMS simples.

Esta Norma Técnica Peruana puede usarse en el ámbito interno y externo de las organizaciones.

0.2 Enfoque de proceso

Esta Norma Técnica Peruana promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, mantener y mejorar la efectividad de un ISMS en la organización.

Una organización debe identificar y administrar varias actividades con el fin de funcionar efectivamente. Cualquier actividad que administre y use recursos para lograr la transformación de entradas en salidas, puede ser considerado un proceso. Con frecuencia la salida de un proceso se convierte en la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su administración se define como un "enfoque de proceso".

El enfoque de proceso alienta a sus usuarios a enfatizar la importancia de:

a) entender los requisitos de seguridad de información de negocios y la necesidad de establecer políticas y objetivos para la seguridad de la información;

b) implementar y operar controles en el contexto de administrar el riesgo total del negocio de una organización;

c) monitorear y revisar el desempeño y efectividad del ISMS; y

d) mejoramiento continuo basado en la medición de objetivos.

El modelo conocido como "Planear-Hacer-Verificar-Actuar" - PDCA (Plan-Do-Check-Act), por sus siglas en inglés, puede aplicarse a todos los procesos ISMS. La Figura 1 ilustra cómo un ISMS toma como entrada los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios genera productos de seguridad de la información (es decir: gestión de la seguridad de la información) que cumple estos requisitos y expectativas. La Figura 1 también ilustra los enlaces en los procesos presentados en los capítulos 4, 5, 6, 7 y 8.

La adopción del modelo PDCA también reflejará los principios como se establecieron en la pautas de OECD (2002)[1] para la gobernabilidad de los sistemas y redes de la seguridad de información. Esta Norma Técnica Peruana provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación.

EJEMPLO 1

Un requisito pudiera ser aquel que las brechas en la seguridad de la información no causen serios daños financieros y/o dañen la imagen de la organización.

EJEMPLO 2

Una expectativa podría ser que si ocurriera un incidente serio – que afecte el web site del negocio de una organización – debe existir personal capacitado en procedimientos adecuados para minimizar el impacto.

[1] OECD Guía para la seguridad de los Sistemas de Información y Redes – Hacia una cultura de seguridad. Paris: OECD, Julio 2002. www.oecd.org

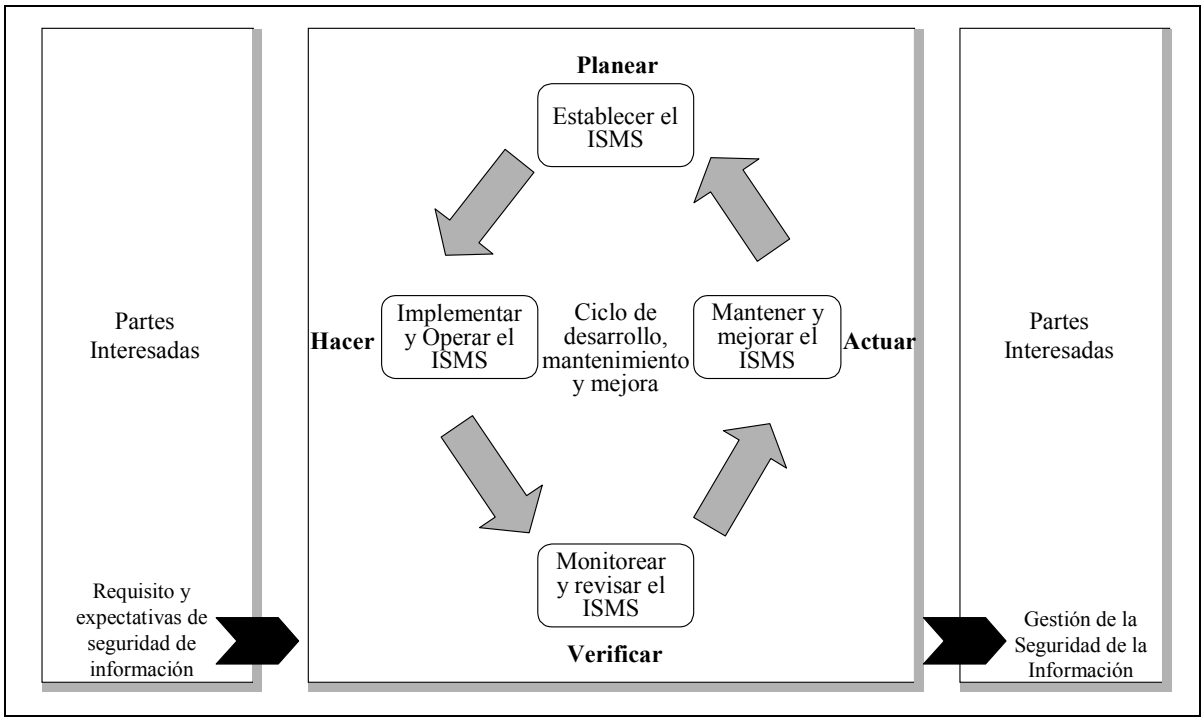

FIGURA 1 – Modelo PDCA aplicado al proceso ISMS

Planear (establecer el ISMS)	Establecer las políticas, objetivos, procesos y procedimientos de seguridad relevantes para administrar el riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos de la organización.
Hacer (implementar y operar el ISMS)	Implementar y operar las políticas, controles, procesos y procedimientos de seguridad.
Verificar (monitorear y revisar el ISMS)	Monitorear y evaluar el funcionamiento de los procesos con respecto a las políticas, objetivos y experiencia práctica de seguridad, informando sobre los resultados obtenidos a la gerencia para su revisión.
Actuar (mantener y mejorar el ISMS)	Tomar acciones correctivas y preventivas basándose en los resultados de la revisión gerencial para alcanzar la mejora continua del ISMS.

0.3 Compatibilidad con otros sistemas de gestión

Esta Norma Técnica Peruana está alineada con la ISO 9001:2000 y la ISO 14001:2004 con el fin de respaldar una implementación y operación consistente e integrada con las normas de gestión afines. Un sistema de gestión convenientemente diseñado puede satisfacer así los requisitos de todos estos estándares. Tabla C.1, ilustra la relación entre los capítulos de esta norma, ISO 9001:2000 y la ISO 14001:2004.

Esta Norma Técnica Peruana está diseñada para hacer posible que una organización se alinee o integre su ISMS con los requisitos de los sistemas de gestión relacionados.

---oooOooo---

EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

IMPORTANTE: Esta Norma Técnica Peruana no pretende incluir todos los términos necesarios para un contrato. Los usuarios son responsables de su correcta aplicación. Cumplir con una norma no confiere en sí mismo inmunidad de las obligaciones legales.

1. ALCANCE

1.1 Aspectos generales

Esta Norma Técnica Peruana cubre todo los tipos de organizaciones (como por ejemplo: empresas comerciales, agencias de gobierno y organizaciones sin fines de lucro). Esta NTP especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS documentado dentro del contexto de los riesgos de negocio de la organización. Especifica los requisitos para implementar los controles de seguridad adaptado a las necesidades individuales de las organizaciones o partes de las mismas.

El ISMS está diseñado para garantizar y proporcionar controles de seguridad adecuados que protejan los activos de información, brindando confianza a las partes interesadas.

NOTA 1: Las referencias de "negocio" en esta Norma Técnica Peruana deben ser interpretadas ampliamente para representar las actividades que son base para los propósitos de la existencia de la organización.

NOTA 2: La ISO/IEC 17799 provee pautas de implementación que pueden ser utilizadas cuando se designen controles.

1.2 Aplicación

Los requisitos establecidos en esta NTP son generales y tienen la intención de aplicarse a todas las organizaciones, sin tomar en cuenta el tipo, tamaño y naturaleza del negocio. Cuando una organización reclama conformidad con esta norma, no es aceptable excluir cualquiera de los requisitos especificados en los capítulos 4, 5, 6, 7 y 8.

Cualquier exclusión de los controles necesarios para satisfacer el criterio de aceptación de los riesgos necesarios, debe justificarse y las necesidades de evidencias que debe ofrecerse en cuanto a que las personas responsables han aceptado adecuadamente los riesgos asociados. Cuando se realiza exclusiones de controles, los reclamos de conformidad de esta NTP no son aceptables a menos que esas exclusiones no afecten la capacidad y/o responsabilidad de la organización para ofrecer seguridad de la información que cumple los requisitos de seguridad establecidos por la evaluación de riesgo y requisitos reglamentarios aplicables.

NOTA: Si una organización ya posee un sistema operativo de gestión de procesos de negocio (por ejemplo en relación con la ISO 9001 o ISO 14001), es preferible, en la mayoría de los casos, satisfacer los requisitos de esta NTP dentro de los sistemas de gestión existentes.

2. REFERENCIAS NORMATIVAS

Las siguientes normas contienen disposiciones que al ser citadas en este texto, constituyen requisitos de esta Norma Técnica Peruana. Las ediciones indicadas estaban en vigencia en el momento de esta publicación. Como toda Norma está sujeta a revisión, se recomienda a aquellos que realicen acuerdos en base a ellas, que analicen la conveniencia de usar las ediciones recientes de las normas citadas seguidamente. El Organismo Peruano de Normalización posee la información de las Normas Técnicas Peruanas en vigencia en todo momento.

2.1 Normas Técnicas Internacionales

2.1.1	ISO/IEC 17799:2005	Information technology – Security techniques - Code of practice for information security management

3. TÉRMINOS Y DEFINICIONES

Para los fines de esta Norma Técnica Peruana, se aplican los siguientes términos y definiciones:

3.1 **activo:** Algo que presenta valor para la organización.
[ISO/IEC 13335-1:2004]

3.2 **disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.
[ISO/IEC 13335-1:2004]

3.3 **confidencialidad:** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.
[ISO/IEC 13335-1:2004]

3.4 **seguridad de la información:** Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.
[ISO/IEC 17799:2005]

3.5 **evento de la seguridad de la información:** Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.
[ISO/IEC TR 18044:2004]

3.6 **incidente de la seguridad de la información:** Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.
[ISO/IEC TR 18044:2004]

3.7 **sistema de gestión de seguridad de la información – ISMS:** Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, 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:** Salvaguardar la exactitud e integridad de la información y activos asociados.
[ISO/IEC TR 13335-1:2004]

3.9 **riesgo residual**: Riesgo remanente después de un tratamiento del riesgo.
[ISO/IEC Guide 73:2002]

3.10 **aceptación del riesgo:** Decisión de aceptar el riesgo.
[ISO/IEC Guide 73:2002]

3.11 **análisis del riesgo:** Uso sistemático de información para identificar amenazas y estimar el riesgo.
[ISO/IEC Guide 73:2002]

3.12 **estimación del riesgo:** Proceso total de análisis y evaluación del riesgo.
[ISO/IEC Guide 73:2002]

3.13 **evaluación del riesgo:** Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.
[ISO/IEC Guide 73:2002]

3.14 **gestión del riesgo:** Actividades coordinadas para dirigir y controlar el riesgo en una organización.
[ISO/IEC Guide 73:2002]

3.15 **tratamiento del riesgo:** Proceso de selección e implementación de controles para minimizar el riesgo.
[ISO/IEC Guide 73:2002]

3.16 **declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles que son relevantes y aplicables al ISMS de la organización.

NOTA: los objetivos y controles están basados en los resultados y conclusiones de los procesos de evaluación del riesgo y tratamiento del riesgo, requisitos legales o regulatorios, obligaciones contractuales y los requisitos de negocio de la información de seguridad de la organización.

4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1 Requisitos generales

La organización desarrollará, implementará, operará, monitoreará, revisará, mantendrá y continuará la mejora de un ISMS documentado dentro del contexto de las actividades y riesgos totales de la organización. Para los fines de esta NTP, el proceso usado se basa en el modelo PDCA mostrado en la Figura 1.

4.2 Establecimiento y administración del ISMS

4.2.1 Establecimiento del ISMS

La organización realizará lo siguiente:

a) Definir el alcance y límites del ISMS en términos de las características del negocio, la organización, su localización, activos y tecnología e incluyendo detalles y justificaciones para cualquier exclusión del alcance (véase 1.2).

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

1) incluye un marco para establecer sus objetivos y establece un sentido total de dirección y principios para acción con miras a la seguridad de la información;
2) considera requisitos de negocios, legales o regulatorios y obligaciones de seguridad contractual;
3) establece el contexto estratégico organizacional y la gestión del riesgo en el cual tiene lugar el establecimiento y mantenimiento del ISMS;
4) establece criterios frente a los cuales se evaluará el riesgo y se definirá la estructura de evaluación del riesgo [véase 4.2.1c)];
5) ha sido aprobado por la gerencia.

NOTA: Para propósitos de esta Norma Técnica Peruana, la política de ISMS es considerada como un conjunto de la política de la seguridad de información. Estas políticas pueden ser descritas en otro documento.

c) Definir un enfoque sistemático para la evaluación del riesgo en la organización.

1) Identificar una metodología de evaluación del riesgo que se adecue al ISMS y a requisitos legales y regulatorios de la información de seguridad del negocio identificada.
2) Determinar criterios para aceptar e identificar los niveles aceptables del riesgo [véase 5.1f].

La metodología de evaluación de riesgos seleccionada debe asegurar que la evaluación de riesgos produzca resultados comparables y reproducibles.

NOTA: Existen diferentes metodologías para una evaluación de riesgos. Los ejemplos de metodologías de evaluación de riesgos son discutidas en la ISO/IEC TR 13335-3.

d) Identificar los riesgos.

1) Identificar los activos dentro del alcance del ISMS y los propietarios[2] de estos activos.
2) Identificar las amenazas a esos activos.
3) Identificar las vulnerabilidades que podrían explotarse mediante estas amenazas.
4) Identificar los impactos de pérdidas de confidencialidad, integridad y disponibilidad sobre los activos.

e) Analizar y Evaluar los riesgos.

1) Evaluar los daños comerciales que podrían resultar de una falla de seguridad, considerando las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
2) Evaluar las posibilidades de falla de seguridad, teniendo en cuenta las amenazas, vulnerabilidades e impactos asociados con estos activos y los controles implementados actualmente.
3) Estimar los niveles de los riesgos.
4) Determinar si el riesgo es aceptable o requiere tratamiento usando el criterio establecido en 4.2.1c)2).

f) Identificar y evaluar opciones para el tratamiento del riesgo.

Las posibles acciones incluyen:

1) aplicar los controles apropiados;
2) aceptar riesgos conciente y objetivamente, siempre y cuando satisfagan claramente la política de la organización y el criterio para la aceptación del riesgo [véase 4.2.1c)2)];
3) evitar riesgos; y
4) transferir los riesgos de negocio asociados a otras partes, por ejemplo: aseguradores, proveedores.

g) Seleccionar objetivos de control y controles para el tratamiento del riesgo.

[2] El termino “propietario” identifica a un individuo o entidad que aprueba la responsabilidad por la gestión por controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona tiene algún derecho de propiedad realmente sobre el activo.

Se seleccionará los objetivos de control y controles adecuados y se justificará en base a las conclusiones de la evaluación y proceso de tratamiento de riesgo. Esta selección debe tomar en cuenta el criterio para aceptación de riesgos [véase 4.2.1c)2)] así como los requisitos legales, regulatorios y contractuales.

Los objetivos de control y controles del Anexo A deben ser seleccionados como parte del proceso así como adecuados para cubrir los requisitos identificados.

Los objetivos de control y los controles que figuran en el Anexo A no son exhaustivos y también puede seleccionarse objetivos de control y controles adicionales.

NOTA: El Anexo A contiene una lista comprensible de objetivos de control que han sido encontrados como relevantes para las organizaciones. Los usuarios de esta NTP son dirigidos a este Anexo A como un punto de partida para la selección de controles con el fin de asegurar que no se hayan obviado opciones de control importantes.

h) Obtener aprobación por parte de la gerencia sobre los riesgos residuales propuestos.

i) Obtener autorización por parte de la gerencia para implementar y operar el ISMS.

j) Prepara una declaración de aplicabilidad.

Una declaración de aplicabilidad debe ser preparada y debe incluir lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1g) y las razones para su selección;
2) los objetivos de control y los controles implementados actualmente [véase 4.2.1e)2)]; y
3) se registrará la exclusión de cualquier objetivo de control y controles que figuran en el Anexo A así como su justificación.

NOTA: La declaración de aplicabilidad provee un resumen de decisiones concernientes a la evaluación de riesgos. Las exclusiones justificadas proveen una verificación cruzada de que ningún control se ha omitido inadvertidamente.

4.2.2 Implementar y operar el ISMS

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgos que identifique la acción administrativa adecuada, 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 con el fin de alcanzar los objetivos de control identificados, que incluyen la consideración de financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1g) para cumplir con los objetivos de control.

d) Definir como medir la efectividad de los controles o grupos de control seleccionados y especificar como estas medidas serán utilizadas para alcanzar la efectividad en el control con el fin de producir resultados comparables y reproducibles [véase 4.2.3c)].

NOTA: Medir la efectividad de los controles permite a los gerentes y al personal determinar que tan bien los controles logran los objetivos de control planeados.

e) Implementar programas de capacitación y concientización (véase 5.2.2).

f) Administrar las operaciones del ISMS.

g) Administrar los recursos para el ISMS (véase 5.2)

h) Implementar procedimientos y otros controles capaces de hacer posible la inmediata detección y respuesta a los incidentes de seguridad (véase 4.2.3a)).

4.2.3 Monitorear y revisar el ISMS

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y otros controles para:

1) detectar inmediatamente errores en los resultados de procesamiento;
2) identificar inmediatamente brechas de seguridad e incidentes;
3) hacer posible que la gerencia determine si las actividades de seguridad delegadas a personas o implementadas mediante el área de tecnología de la información se realizan de acuerdo a lo planeado;
4) ayudar a detectar eventos de seguridad y desde ahí prevenir los incidentes de seguridad mediante el uso de indicadores; y
5) determinar si las acciones realizadas para resolver una violación de seguridad fueron efectivas.

b) Emprender revisiones regulares de la efectividad del ISMS (incluyendo cumplir con la política de seguridad, objetivos y revisar los controles de seguridad) considerando los resultados de auditorías de seguridad, incidentes, sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la efectividad de los controles para verificar que se tomaron en cuenta los requisitos de seguridad.

d) Revisar la evaluación de riesgos en intervalos planificados y revisar el nivel del riesgo residual y riesgo aceptable, tomando en cuenta los cambios a:

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

e) Realizar auditorías internas de ISMS en intervalos planificados (véase el capítulo 6).

NOTA: Las auditorías internas son conducidas por, o a favor de, la misma organización, para propósitos internos.

f) Emprender un revisión administrativa del ISMS en una base para garantizar que el alcance siga siendo el adecuado y las mejoras al proceso ISMS sean identificadas (Véase 7.1).

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

h) Registrar acciones y eventos que podrían tener un impacto en la efectividad o funcionamiento del ISMS (véase 4.3.3).

4.2.4 Mantener y mejorar el ISMS

La organización debe regularmente hacer lo siguiente:

a) Implementar en el ISMS las mejoras identificadas.

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

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

d) Garantizar que las mejoras alcancen sus objetivos planificados.

4.3 Requisitos de documentación

4.3.1 Aspectos generales

La documentación debe incluir registros de la decisiones gerenciales, asegurar que las acciones sean trazables a estas decisiones y a las políticas y asegurar que los resultados grabados son reproducibles.

Es importante ser capaz de demostrar la relación de los controles seleccionados con los resultados de la evaluación de riesgos y el proceso de tratamiento de riesgos así como subsecuentemente a las políticas y objetivos de ISMS.

La documentación del ISMS deberá incluir lo siguiente:

a) Declaraciones documentadas de la política de seguridad (véase 4.2.1b)) y objetivos;

b) el alcance del ISMS (véase 4.2.1a));

c) los procedimientos y controles que soportan el ISMS;

d) una descripción de la metodología de evaluación del riesgo (véase 4.2.1c));

e) informe de evaluación del riesgo (véase 4.2.1c) a 4.2.1g));

f) plan de tratamiento del riesgo (véase 4.2.2b));

g) procedimientos documentados necesarios en la organización para garantizar la planificación efectiva, funcionamiento y control de sus procesos de seguridad de la información y describir como medir la efectividad de los controles (véase 4.2.3c));

h) registros exigidos por esta NTP (véase 4.3.3); y

i) declaración de aplicabilidad.

NOTA 1: Cuando aparece el término "procedimiento documentado" dentro de esta norma, significa que el procedimiento está establecido, documentado, implementado y mantenido.

NOTA 2: La extensión de la documentación del ISMS puede diferir de una organización a otra dependiendo de:
- El tamaño de la organización y el tipo de actividades; y
- El alcance y complejidad de los requisitos de seguridad y del sistema a ser administrado.

NOTA 3: Los documentos y registros pueden tener cualquier forma y tipo de medio.

4.3.2 Control de documentos

Los documentos exigidos por el ISMS estarán protegidos y controlados. Se establecerá un procedimiento documentado para definir las acciones administrativas necesarias para:

a) aprobar documentos para su adecuación antes de la emisión;

b) revisar y actualizar los documentos que sean necesarios y reaprobar documentos;

c) asegurar que los cambios y el estado de la versión actual de los documentos sean identificados;

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

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

f) asegurar que los documentos se encuentren disponibles para quienes los necesiten y sean transferidos, almacenados y dispuestos en concordancia con los procedimientos aplicables a su clasificación;

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

h) asegurar que la distribución de documentos sea controlada;

i) prevenir el uso no intencional de documentos obsoletos; y

j) aplicar la identificación adecuada de estos si se guardan para algún propósito.

4.3.3 Control de registros

Se establecerán y mantendrán registros para ofrecer evidencia de conformidad con los requisitos y el funcionamiento efectivo del ISMS. Estos registros deberán ser controlados. El ISMS tomará en cuenta cualquier requisito legal pertinente. Los registros deben ser legibles, fácilmente identificables y accesibles. Los controles necesarios para la identificación, almacenamiento, protección, acceso, tiempo de retención y disposición de registros deberán ser implementados y documentados.

Se mantendrán los registros del rendimiento del proceso como se señala en 4.2 y de todos los incidentes de seguridad relacionados con el ISMS.

EJEMPLO:

Ejemplos de registros son los libros de visitantes, reportes de auditoría y autorización de acceso.

5. RESPONSABILIDAD DE LA GERENCIA

5.1 Compromiso de la gerencia

La gerencia entregará evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del ISMS mediante:

a) estableciendo una política del ISMS;

b) asegurando que los objetivos y planes del ISMS sean establecidos;

c) estableciendo los roles y responsabilidades para la seguridad de la información;

d) comunicando a la organización la importancia del cumplimiento de los objetivos de seguridad de la información y de acuerdo a la política de seguridad de la información, sus responsabilidades de acuerdo a ley y la necesidad de una mejora continua;

e) brindando recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el ISMS (véase 5.2.1);

f) decidiendo el criterio para aceptación de riesgos y el nivel de riesgo aceptable;

g) asegurar que las auditorías internas del ISMS sean realizadas (véase capitulo 6); y

h) realizando revisiones gerenciales del ISMS (véase capítulo 7).

5.2 Administración de recursos

5.2.1 Provisión de recursos

La organización deberá determinar y brindar los recursos necesarios para:

a) establecer, implementar, hacer funcionar y mantener el ISMS;

b) asegurar que los procedimientos de seguridad de la información respalden los requisitos de negocio;

c) identificar y atender los requisitos legales y regulatorios, obligaciones de seguridad contractuales;

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

e) llevar a cabo revisiones necesarias y aplicar las medidas correspondientes según los resultados de estas revisiones;

f) cuando sea necesario, mejorar la efectividad del ISMS.

5.2.2 Capacitación, concientización y competencia

La organización deberá asegurar que todo el personal al cual se le asigna responsabilidades definidas en el ISMS sea competente para realizar las tareas requeridas mediante:

a) determinando las aptitudes necesarias del personal que lleva a cabo labores vinculadas al ISMS;

b) ofreciendo capacitación o tomando otras acciones (por ejemplo empleando personal idóneo) para satisfacer estas necesidades;

c) evaluando la efectividad de la capacitación ofrecida y las acciones ejecutadas; y

d) manteniendo registros de educación, capacitación, habilidades, experiencia y calificaciones (véase 4.3.3).

La organización también debe garantizar que todo el personal pertinente tome conciencia de la relevancia e importancia de las actividades de seguridad de la información y cómo estas contribuyen al logro de los objetivos del ISMS.

6. AUDITORÍAS INTERNAS DEL ISMS

La organización conducirá auditorías internas del ISMS a intervalos periódicos para determinar si los objetivos de control, controles, procesos y procedimientos identificados de su ISMS:

a) están conformes a los requisitos de esta NTPy legislación o reglamentos relevantes;

b) están conformes con los requisitos de seguridad de la información identificados;

c) se han implementado y mantenido efectivamente; y

d) funcionan como se espera.

Un programa de auditoría debe planificarse tomando en consideración la condición e importancia de los procesos y áreas a auditarse, así como los resultados de auditorías previas. Deberá definirse los criterios, alcance, frecuencia y métodos de las auditorías. La selección de auditores y conducción de auditorías deben garantizar objetividad e imparcialidad en el proceso de auditoría. Los auditores no deben auditar su propio trabajo.
Las responsabilidades y requisitos para la planificación y conducción de auditorías y la información de los resultados y mantenimiento de registros (véase 4.3.3) deberán definirse en un procedimiento documentado.

La gerencia responsable del área que está bajo auditoría garantizará que las acciones se ejecuten sin retrasos indebidos, con el fin de eliminar las no conformidades detectadas y sus causas. Las actividades de mejora incluyen la verificación de las acciones tomadas y el reporte de los resultados de verificación (véase capítulo 8).

NOTA: ISO 19011:2002, Guía para la calidad y/o gestión de sistemas de auditoría del medio ambiente, pueden proveer una guía útil para llevar a cabo una auditoría ISMS interna.

7. REVISIÓN GERENCIAL DEL ISMS

7.1 Aspectos generales

La gerencia revisará el ISMS de la organización a intervalos planificados (al menos una vez por año) para garantizar su idoneidad continua, adecuación y efectividad. Esta revisión debe incluir las oportunidades de evaluación para mejora y la necesidad de cambios al ISMS incluyendo la política y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se mantendrán registros sobre las mismas (véase el apartado 4.3.3).

7.2 Revisión: entradas

La revisión gerencial deberá incluir la información de entrada siguiente:

a) resultados de las auditorías y revisiones del ISMS;

b) retroalimentación de las partes interesadas;

c) técnicas, productos o procedimientos que podrían usarse en la organización para mejorar el funcionamiento y efectividad del ISMS;

d) situación de las acciones preventivas y correctivas;

e) vulnerabilidad o amenazas no atendidas adecuadamente en la evaluación previa del riesgo;

f) resultados de las medidas efectivas;

g) acciones de seguimiento de las revisiones gerenciales previas;

h) cualquier cambio que podría afectar el ISMS; y

i) recomendaciones para mejoras.

7.3 Revisión: salidas

La revisión gerencial incluirá cualquier decisión y acción relacionada con lo siguiente:

a) Mejora de la efectividad del ISMS.

b) Actualizaciones de la evaluación de riesgos y del plan de tratamiento de riesgo.

c) Modificación de los procedimientos y controles vinculados con la seguridad de la información, según sea necesario para responder a los eventos internos y externos que pueden impactar en el ISMS, incluyendo cambios a:

1) requisitos de negocio;
2) requisitos de seguridad;
3) procesos de negocio que afectan los requisitos de negocio existentes;
4) marco regulatorio o legal;
5) obligaciones contractuales; y
6) niveles de riesgo y/o criterios de aceptación de riesgos.

d) Necesidades de recursos.

e) Mejoras en como se mide la efectividad de los controles;

8. MEJORA DEL ISMS

8.1 Mejora continua

La organización mejorará continuamente la efectividad de los ISMS a través del uso de la política de seguridad de la información, objetivos de seguridad, resultados de auditorías, análisis de eventos monitoreados, acciones correctivas y preventivas, y revisión gerencial (véase capitulo 7).

8.2 Acciones correctivas

La organización tomará acciones para eliminar la causa de las no conformidades asociadas con la implementación y operación del ISMS con el fin de prevenir recurrencias. Los procedimientos documentados para las acciones correctivas se definirán como requisitos para:

a) identificación de 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 producirse;

d) determinar e implementar la acción correctiva necesaria;

e) registrar los resultados de las acciones tomadas (véase 4.3.3); y

f) revisar las acciones correctivas tomadas.

8.3 Acciones preventivas

La organización determinará las acciones para eliminar las causas potenciales no conformidades con los requisitos de ISMS con el fin de prevenir su ocurrencia. Las acciones preventivas deberán ser adecuadas al impacto de los problemas potenciales. El procedimiento documentado para las acciones preventivas definirá los requisitos para:

a) identificar las no conformidades potenciales y sus causas;

b) evaluar la necesidad de una acción con el fin de prevenir ocurrencias de no conformidades;

c) determinar e implementar las acciones preventivas necesarias;

d) registrar los resultados de las acciones tomadas (véase 4.3.3) y

e) revisar las acciones preventivas tomadas;

La organización debe identificar los riesgos alterados e identificar los requisitos de acciones preventivas centrándose en aquellos significativamente alterados.

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

NOTA: Las acciones para prevenir no conformidades con frecuencia son más económicas que las acciones correctivas.

9. ANTECEDENTES

9.1.	ISO/IEC 27001:2005	Information technology – Security techniques – Information security management systems – Requirements
9.2.	NTP 821.101: 2005	EDI. Sistemas de gestión de seguridad de la información – Especificaciones con guía de uso

ANEXO A
(NORMATIVO)

OBJETIVOS DE CONTROL Y CONTROLES

Los objetivos de control y los controles que figuran en la tabla A.1 se derivan y alinean directamente con los que figuran en NTP-ISO/IEC 17799:2007, capítulos 5 a 15. Las listas en estas tablas no son exhaustivas y la organización puede 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 ISMS especificado en 4.2.1.

La NTP-ISO/IEC 17799:2006, capítulos 5 a 15 ofrecen asesoría de implementación y pautas sobre las mejores prácticas en apoyo de los controles especificados de 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 de control:* Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos del negocio, las leyes y las regulaciones.		
A.5.1.1	*Documentos de política de seguridad de la información*	Control La gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieran.
A.5.1.2	*Revisión de la política de seguridad de información*	Control La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva.

A.6 Seguridad organizacional

A.6.1 Organización interna *Objetivo de control:* Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	*Comité de Gestión de seguridad de la información*	Control La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de responsabilidades de la seguridad de información.
A.6.1.2	*Coordinación de la seguridad de la información*	Control Las actividades en la seguridad de información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo.
A.6.1.3	*Asignación de responsabilidades sobre seguridad de la información*	Control Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.
A.6.1.4	*Proceso de autorización para las nuevas instalaciones de procesamiento de información*	Control Debe establecerse y definirse un proceso de gestión de autorización para facilitar los nuevos procesamientos información.
A.6.1.5	*Acuerdos de confidencialidad*	Control Se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información.
A.6.1.6	*Contacto con autoridades*	Control Se debe mantener contactos apropiados con las autorizaciones relevantes.
A.6.1.7	*Contacto con grupos de interés especial*	Control Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales.
A.6.1.8	*Revisión independiente de seguridad de la información*	Control El alcance de la organización para manejar la seguridad de información, así como su implementación (como por ejemplo: los objetivos de control, los controles, las políticas, procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.

A.6.2 Seguridad del acceso a terceras partes *Objetivo de control:* Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros.		
A.6.2.1	*Identificación de riesgos por el acceso de terceros*	Control Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados antes de permitir su acceso.
A.6.2.2	*Requisitos de seguridad cuando se trata con clientes*	Control Se deben identificar todos los requisitos de seguridad antes de dar acceso a clientes a los activos o a la información de la organización.
A.6.2.3	*Requisitos de seguridad en contratos con terceros*	Control Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones deben cubrir todos los requisitos de seguridad necesarios.

A.7 Gestión de activos

A.7.1 Responsabilidad por los activos *Objetivo de control:* Mantener la protección apropiada de los activos de la organización.		
A.7.1.1	*Inventario de activos*	Control Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente identificados.
A.7.1.2	*Propiedad de los activos*	Control Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad[3] de una parte designada de la organización.
A.7.1.3	*Uso aceptable de los activos*	Control Se deben de identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones de procesamiento de información.

[3] El termino "propietario" identifica a un individuo o entidad que aprueba la responsabilidad por la gestión por controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona tiene algún derecho de propiedad realmente sobre el activo.

A.7.2 Clasificación de la información *Objetivo de control:* Asegurar que los activos de información reciban un nivel de protección adecuado.		
A.7.2.1	*Guías de clasificación*	Control La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	*Etiquetado y tratamiento de la información*	Control Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información de conformidad con el esquema de clasificación adoptado por la organización.

A.8 Seguridad en recursos humanos

A.8.1 Previo al empleo[4] *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han sido considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones.		
A.8.1.1	*Roles y responsabilidades*	Control Se definirán y documentarán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización.
A.8.1.2	*Investigación*	Control Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleos, contratistas y personal externo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos.
A.8.1.3	*Términos y condiciones de la relación laboral*	Control Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.

[4] Explicación: la palabra "empleo" se utiliza aquí para cubrir las siguientes situaciones diferentes: empleo de las personas (temporalmente o durante largo tiempo), designando roles de trabajo, cambiando roles de trabajo, asignando contratos, y la terminación de cualquiera de estos arreglos.

A.8.2 Durante el empleo *Objetivo de control:* Asegurar que todos los empleados, contratistas y usuarios externos sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para aplicar la política de seguridad de la organización en el curso de trabajo normal y reducir el riesgo de error humano.		
A.8.2.1	*Gestión de responsabilidades*	Control La gerencia debe requerir a los empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y procedimientos de la organización.
A.8.2.2	*Concientización, educación y entrenamiento en la seguridad de información*	Control Todos los empleados de la organización y, donde sea relevante, contratistas y usuarios externos deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
A.8.2.3	*Proceso disciplinario*	Control Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad.
A.8.3 Finalización o cambio de empleo *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada.		
A.8.3.1	*Responsabilidades de finalización*	Control Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados tan pronto como sea posible.
A.8.3.2	*Devolución de activos*	Control Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo.
A.8.3.3	*Retiro de los derechos de acceso*	Control El derecho de acceso a la información y a las instalaciones de procesamiento de información, que se le otorga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios.

A.9 Seguridad física y del entorno

A.9.1 Áreas seguras *Objetivo de control:* Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización.		
A.9.1.1	*Seguridad física perimetral*	Control Las organizaciones usarán perímetros de seguridad (barreras como paredes, puertas con control de entrada por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información.
A.9.1.2	*Controles físicos de entradas*	Control Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que únicamente personal autorizado pueda ingresar.
A.9.1.3	*Seguridad de oficinas, despachos y recursos*	Control Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.
A.9.1.4	*Protección contra amenazas externas y ambientales*	Control Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.
A.9.1.5	*El trabajo en las áreas seguras*	Control Se debe designar y mantener protección física y pautas para trabajar en áreas seguras.
A.9.1.6	*Áreas de carga, descarga y acceso público*	Control Las áreas de carga, descarga y acceso público y otras áreas donde las personas tengan acceso deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado.

A.9.2 Seguridad de los equipos *Objetivo de control:* Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.		
A.9.2.1	*Ubicación y protección de equipos*	Control El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidades de acceso no autorizado.
A.9.2.2	*Suministro eléctrico*	Control El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.
A.9.2.3	*Seguridad del cableado*	Control Se protegerá el cableado de energía y telecomunicaciones que transportan datos o respaldan servicios de información frente a interceptaciones o daños.
A.9.2.4	*Mantenimiento de equipos*	Control El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad.
A.9.2.5	*Seguridad de equipos fuera de los locales de la organización*	Control Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.
A.9.2.6	*Seguridad en el re-uso o eliminación de equipos*	Control Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y los software con licencia han sido removidos o sobrescritos antes de desecharlos o reutilizarlos.
A.9.2.7	*Retiro de propiedad*	Control Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.

A.10 Gestión de comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades de operación *Objetivo de control:* Asegurar la operación correcta y segura de los recursos de procesamiento de información.		
A.10.1.1	*Documentación de procedimientos operativos*	Control Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.
A.10.1.2	*Gestión de cambios*	Control Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.
A.10.1.3	*Segregación de tareas*	Control Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización.
A.10.1.4	*Separación de las instalaciones de desarrollo, prueba y operación*	Control Se separarán las instalaciones de desarrollo, prueba y operación con el fin de reducir el riesgo de acceso no autorizado o cambios en el sistema operacional.
A.10.2 Gestión de entrega de servicios externos *Objetivo de control:* Implementar y mantener un nivel apropiado de seguridad de información y servicios de entrega en concordancia con los acuerdos de servicios de entrega por parte de terceros.		
A.10.2.1	*Entrega de servicios*	Control Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, estén operativos y sean mantenidos por el personal externo.
A.10.2.2	*Monitoreo y revisión de los servicios externos*	Control Los servicios, reportes, y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben de llevar a cabo auditorías con regularidad.

A.10.2.3	*Gestión de cambios de los servicios externos*	Control Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de la política de seguridad de información, procedimientos y controles, tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevaluación de riesgos.
A.10.3 Planificación y aceptación del sistema *Objetivo de control:* Minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	*Gestión de la capacidad*	Control Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requisitos de capacidad para asegurar el desarrollo requerido por el sistema.
A.10.3.2	*Aceptación del sistema*	Control Se establecerán los criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de la aceptación.
A.10.4 Protección contra software malicioso *Objetivo de control:* Proteger la integridad del software y de la información.		
A.10.4.1	*Controles contra software malicioso*	Control Para ofrecer protección frente a software malicioso, se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.
A.10.4.2	*Controles contra software móvil*	Control Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida. Igualmente, se debe prevenir la ejecución de código móvil no autorizado.
A.10.5 Gestión interna de respaldo y recuperación *Objetivo de control:* Mantener la integridad y disponibilidad del procesamiento de información y servicios de comunicación.		
A.10.5.1	*Recuperación de la información*	Control Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada.

A.10.6 Gestión de seguridad de redes *Objetivo de control:* Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	*Controles de red*	Control Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la seguridad de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.
A.10.6.2	*Seguridad de los servicios de red*	Control Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sean provistos interna o externamente.
A.10.7 Utilización y seguridad de los medios de información *Objetivo de control:* Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio.		
A.10.7.1	*Gestión de medios removibles*	Control Deben de existir procedimientos para la gestión de medios removibles.
A.10.7.2	*Eliminación de medios*	Control Se eliminarán los medios de forma segura cuando ya no se necesiten, utilizando procedimientos formales.
A.10.7.3	*Procedimientos de manipulación de la información*	Control Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso.
A.10.7.4	*Seguridad de la documentación de sistemas*	Control La documentación de los sistemas se protegerá de accesos no autorizados.

A.10.8 Intercambio de información *Objetivo de control:* Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas.		
A.10.8.1	*Políticas y procedimientos para el intercambio de información*	Control Se deben establecer políticas, procedimientos y controles para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación.
A.10.8.2	*Acuerdos de intercambio*	Control Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	*Seguridad de medios físicos en tránsito*	Control Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de los límites físicos de la organización.
A.10.8.4	*Seguridad del correo electrónico*	Control La información contenida en correos electrónicos debe ser protegida apropiadamente.
A.10.8.5	*Seguridad en los 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 del negocio.
A.10.9 Servicios de comercio electrónico *Objetivo de control:* Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso.		
A.10.9.1	*Seguridad en comercio electrónico*	Control El comercio electrónico será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o modificación de información.
A.10.9.2	*Seguridad en las transacciones en línea*	Control La información contenida en las transacciones en línea debe ser protegida para prevenir transmisiones incompletas, rutas incorrectas, alteración no autorizada de mensajes, o duplicación no autorizada de mensajes.
A.10.9.3	*Información disponible públicamente*	Control Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas.

A.10.10 Monitoreo *Objetivo de control:* Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoría*	Control Se deben producir y guardar, por un periodo acordado, los registros de auditoría que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente.
A.10.10.3	*Protección de la información de registro*	Control Las instalaciones e información de registro debe ser protegido contra acceso forzado y no autorizado.
A.10.10.4	*Registros de administrador y operador*	Control Las actividades del administrador y operadores deben ser registradas.
A.10.10.5	*Registros con faltas*	Control Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas.
A.10.10.6	*Sincronización de reloj*	Control Los relojes de todos los sistemas relevantes de procesamiento de información dentro de la organización deben estar sincronizados con una fuente de tiempo actual acordado.

A.11 Control de accesos

A.11.1 Requisitos de negocio para el control de accesos *Objetivo de control:* Controlar los accesos a la información.		
A.11.1.1	*Política de control de accesos*	Control Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.

A.11.2 Gestión de acceso de usuarios *Objetivo de control:* Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.		
A.11.2.1	*Registro de usuarios*	Control Habrá un procedimiento de registro y anulación formal de usuarios para otorgar y eliminar el acceso a todos los servicios y sistemas de información.
A.11.2.2	*Gestión de privilegios*	Control Se restringirá y controlará la asignación y uso de privilegios.
A.11.2.3	*Gestión de contraseñas de usuario*	Control Se controlará la asignación de contraseñas a través de un proceso de gestión formal.
A.11.2.4	*Revisión de los derechos de acceso de los usuarios*	Control La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso del usuario.
A.11.3 Responsabilidades de los usuarios *Objetivo de control:* Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento.		
A.11.3.1	*Uso de contraseñas*	Control Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
A.11.3.2	*Equipo informático de usuario desatendido*	Control Se exige al usuario que asegure protección adecuada a un equipo desatendido.
A.11.3.3	*Política de pantalla y escritorio limpio*	Control Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para las instalaciones de procesamiento de información.
A.11.4 Control de acceso a la red *Objetivo de control:* Prevenir el acceso no autorizado a los servicios de red.		
A.11.4.1	*Política de uso de los servicios de la red*	Control Los usuarios deben tener acceso directo únicamente a los servicios cuyo uso está específicamente autorizado.
A.11.4.2	*Autenticación de usuarios para conexiones externas*	Control Deben usarse apropiados métodos de autenticación para controlar el acceso de usuarios remotos.

A.11.4.3	*Autenticación de equipos en la red*	Control Se debería considerar equipos con identificación automática para autentificar conexiones desde ubicaciones y equipos específicos.
A.11.4.4	*Protección para la configuración de puertos y diagnóstico remoto*	Control Debe controlarse la seguridad en el acceso lógico y físico para el diagnóstico y configuración de puertos.
A.11.4.5	*Segregación en las redes*	Control Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
A.11.4.6	*Control de conexión a las redes*	Control La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la política de control de acceso y los requisitos de las aplicaciones de negocio (véase 11.1).
A.11.4.7	*Control de enrutamiento en la red*	Control Se deben implementar controles de ruteo para asegurar que las conexiones de computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocios.
A.11.5 Control de acceso al sistema operativo *Objetivo de control:* Prevenir accesos no autorizados a los sistemas operativos.		
A.11.5.1	*Procedimientos seguros de conexión*	Control Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información.
A.11.5.2	*Identificación y autenticación del usuario*	Control Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario.
A.11.5.3	*Sistema de gestión de contraseñas*	Control Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.
A.11.5.4	*Uso de los programas utilitarios del sistema*	Control Se debe registrar y controlar firmemente el uso de programas utilitarios que puedan ser capaces de forzar el sistema y los controles de aplicación.

A.11.5.5	*Desconexión automática de terminales*	Control Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.
A.11.5.6	*Limitación del tiempo de conexión*	Control Se usará restricciones de tiempos de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones e información *Objetivo de control:* Evitar el acceso no autorizado a la información contenida en los sistemas.		
A.11.6.1	*Restricción de acceso a la información*	Control El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos con la política de control de acceso.
A.11.6.2	*Aislamiento de sistemas sensibles*	Control Los sistemas sensibles tendrán un ambiente de computo dedicado (aislado).
A.11.7 Informática móvil y teletrabajo *Objetivo de control:* Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo.		
A.11.7.1	*Informática y comunicaciones móviles*	Control Se pondrá en práctica una política formal y se adoptarán los controles adecuados para protegerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación.
A.11.7.2	*Teletrabajo*	Control Se desarrollarán e implementaran políticas, procedimientos y estándares para las actividades de teletrabajo.

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

***A.12.1 Requisitos de seguridad de los sistemas* de información** *Objetivo de seguridad:* Garantizar que la seguridad esté incluida dentro de los sistemas de información.		
A.12.1.1	*Análisis y especificación de los requisitos de seguridad*	Control Los requisitos de negocios para nuevos sistemas, o ampliaciones de los sistemas existentes, especificarán los requisitos de control.

A.12.2 Proceso correcto en aplicaciones *Objetivo de control:* Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones.		
A.12.2.1	*Validación de los datos de entrada*	Control Se validará el ingreso de datos a los sistemas de aplicación para asegurar que sean correctos y adecuados.
A.12.2.2	*Control del proceso interno*	Control Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados.
A.12.2.3	*Integridad de mensajes*	Control Se deben identificar requisitos para la autenticación y protección de la integridad de mensajes. Igualmente, se deben implementar e identificar controles apropiados.
A.12.2.4	*Validación de los datos de salida*	Control Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos *Objetivo de control:* Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.		
A.12.3.1	*Política de uso de los controles criptográficos*	Control Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.
A.12.3.2	*Gestión de claves*	Control Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnica criptográficas dentro de la organización.
A.12.4 Seguridad de los archivos del sistema *Objetivo de control:* Asegurar la seguridad de los archivos del sistema.		
A.12.4.1	*Control del software en producción*	Control Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales.
A.12.4.2	*Protección de los datos de prueba del sistema*	Control Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente.

A.12.4.3	*Control de acceso a la librería de programas fuente*	Control El acceso a las librerías de programas fuente debe ser restringido.
A.12.5 Seguridad en los procesos de desarrollo y soporte *Objetivo de control:* Mantener la seguridad del software de aplicación y la información.		
A.12.5.1	*Procedimientos de control de cambios*	Control La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	*Revisión técnica de los cambios en el sistema operativo*	Control Cuando los sistemas operativos son cambiados, se deben de revisar y probar las aplicaciones criticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.
A.12.5.3	*Restricciones en los cambios a los paquetes de software*	Control No se debe fomentar las modificaciones en los paquetes. Se debe limitar a cambios necesarios y todos estos cambios deben ser estrictamente controlados.
A.12.5.4	*Fuga de información*	Control Se deben de prevenir las oportunidades de fuga de información.
A.12.5.5	*Desarrollo externo del software*	Control La organización debe supervisar y monitorear el desarrollo externo de software.
A.12.6 Gestión de vulnerabilidades técnicas *Objetivo de control:* Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	*Control de vulnerabilidades técnicas*	Control Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas al riesgo.

A.13 Gestión de incidentes en la seguridad de información

A.13.1 Reportando eventos y debilidades en la seguridad de información *Objetivo de control:* Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de manera tal que permitan tomar una acción correctiva a tiempo.		
A.13.1.1	*Reportando eventos de la seguridad de información*	Control Los eventos en la seguridad de información deben ser reportados lo mas rápido posible a través de canales apropiados.
A.13.1.2	*Reportando debilidades de seguridad*	Control Todos los empleados, contratistas o personal externo usuario de los sistemas y servicios de información, deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios.
A.13.2 Gestión de los incidentes y mejoras en la seguridad de información *Objetivo de control:* Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información.		
A.13.2.1	*Responsabilidades y procedimientos*	Control. Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información.
A.13.2.2	*Aprendiendo de los incidentes en la seguridad de información*	Control Deben existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.
A.13.2.3	*Recolección de evidencia*	Control Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información involucre una acción legal (civil o criminal), se debe de recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción.

A.14 Gestión de la continuidad del negocio

A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de información *Objetivo de control:* Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	*Incluyendo la seguridad de la información en la gestión de la continuidad del negocio*	Control Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de la información.
A.14.1.2	*Continuidad del negocio y evaluación de riesgos*	Control Los eventos que pueden causar interrupciones en los procesos del negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	*Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información*	Control Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.
A.14.1.4	*Marco de planificación de la continuidad del negocio*	Control Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades de prueba y mantenimiento.
A.14.1.5	*Probando, manteniendo y reevaluando los planes de continuidad del negocio*	Control Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos.

A.15 Cumplimiento

A.15.1 Cumplimiento de los requisitos legales *Objetivo de control:* Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de cualquier requisito de seguridad.		
A.15.1.1	*Identificación de la legislación aplicable*	Control Se definirán y documentarán explícitamente todos los requisitos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información y la organización.
A.15.1.2	*Derechos de propiedad intelectual (DPI)*	Control Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario.
A.15.1.3	*Salvaguarda de los registros de la organización*	Control Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.
A.15.1.4	*Protección de los datos y privacidad de la información personal*	Control Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales.
A.15.1.5	*Prevención en el mal uso de las instalaciones de procesamiento de la información*	Control Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para propósitos no autorizados.
A.15.1.6	*Regulación de los controles criptográficos*	Control Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos.

A.15.2 Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico *Objetivo de control:* Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.		
A.15.2.1	*Cumplimiento con los estándares y la política de seguridad*	Control Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad.
A.15.2.2	*Comprobación del cumplimiento técnico*	Control Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información.
A.15.3 Consideraciones sobre la auditoría de sistemas *Objetivo de control:* Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.		
A.15.3.1	*Controles de auditoría de sistemas*	Control Se planificarán cuidadosamente las auditorías de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos de negocio.
A.15.3.2	*Protección de las herramientas de auditoría de sistemas*	Control Se protegerá el acceso a las herramientas de auditoría del sistema para prevenir cualquier posible mal uso o daño.

ANEXO B
(INFORMATIVO)

PRINCIPIOS OECD Y ESTA NORMA

Los principios dados en las Pautas OECD para la Seguridad de los Sistemas y Redes de Información se aplican a todos los niveles políticos y operativos que rigen la seguridad de los sistemas de información y redes. Esta NTP ofrece un marco para el sistema de gestión de la seguridad de la información para implementar algunos de los principios OECD usando el modelo PDCA y los procesos descritos en los capítulos 4, 5, 6, y 8 como se indica en la Tabla B.1

TABLA B.1 - Principios OECD y modelo PDCA

Principio OECD	Proceso ISMS y fase PDCA correspondiente
Conocimiento Los participantes deben estar concientes de la necesidad de seguridad de los sistemas y redes de información y lo que pueden hacer para mejorar la seguridad.	Esta actividad es parte de la fase **Hacer** (véase 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** (véase 4.2.2 y **5.1**).
Respuesta Los participantes deben actuar de manera puntual y cooperativa para prevenir, detectar y responder a los incidentes de seguridad.	Esto es parte de la actividad de monitoreo de la fase **Verificar** (véase 4.2.3 y 6 a 7.3) y una actividad de respuesta de la fase **Actuar** (véase 4.2.4 y 8.1 a 8.3). También puede cubrirse con varios aspectos de las fases **Planear** y **Verificar**.
Evaluación del riesgo Los participantes deben conducir evaluaciones del riesgo.	Esta actividad es parte de la fase **Planear** (véase 4.2.1) y evaluación de riesgo es parte de la fase **Verificar** (véase 4.2.3 y 6 a 7.3).

TABLA B.1 - Principios OECD y modelo PDCA *(Fin)*

Principio OECD	Proceso ISMS y fase PDCA correspondiente
Diseño e implementación de seguridad Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.	Una vez que se ha completado la evaluación del riesgo, se ha seleccionado controles para el tratamiento de riesgos como parte de la fase **Planear** (véase 4.2.1). La fase **Hacer** (véase 4.2.2 y 5.2) entonces cubre la implementación y uso operacional de estos controles.
Gestión de seguridad Los participantes deben adoptar un enfoque comprensivo de la gestión de seguridad.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta frente a incidentes, mantenimiento en curso, revisión y auditoría. Todos estos aspectos están incluidos en las fases **Planear**, **Hacer**, **Verificar** y **Actuar**.
Reevaluación Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información y hacer modificaciones adecuadas a las políticas, prácticas, medidas y procedimientos de seguridad	Reevaluación de la seguridad de la información es parte de la fase **Verificación** (véase 4.2.3 y 6 a 7.3) donde debe realizarse revisiones regulares para verificar la efectividad de los sistemas de gestión de seguridad de la información y mejorar la seguridad es parte de la fase **Actuar** (véase 4.2.4 y 8.1 a 8.3)

ANEXO C
(INFORMATIVO)

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

La tabla C.1 muestra la correspondencia entre la norma ISO 9001:2000, ISO 14001:2004 y esta NTPperuana

TABLA C.1 – Correspondencia entre ISO 9001:2000, ISO 14001:2004 y esta Norma

Norma Peruana	ISO 9001:2000	ISO 14001:2004
0 Introducción 0.1 Aspectos Generales 0.2 Enfoque de proceso 0.3 Compatibilidad con otros sistemas de gestión	**0 Introducción** 0.1 Aspectos Generales 0.1 Alcance del proceso 0.2 Relaciones con ISO 9004 0.3 Compatibilidad con otros sistemas de gestión	**Introducción**
1 Alcance 1.1 Aspectos Generales 1.2 Aplicación	**1 Alcance** 1.1 Aspectos Generales 1.2 Aplicaciones	**1 Alcance**
2 Referencias normativas	**2 Referencias normativas**	**2 Referencias normativas**
3 Términos y definiciones	**3 Términos y definiciones**	**3 Términos y definiciones**

Norma Peruana	ISO 9001:2000	ISO 14001:2004
4 Sistema de gestión de seguridad de la información 4.1 Requisitos generales 4.2 Establecimiento y administración de ISMS 4.2.1 Establecimiento de ISMS 4.2.2 Implementar y operar el ISMS 4.2.3 Monitorear y revisar el ISMS 4.2.4 Mantener y mejorar el ISMS	**4 Sistema de gestión de calidad** 4.1 Requisitos generales 8.2.3 Monitoreo y medición de los procesos 8.2.4 Monitoreo y medición del producto	**4 Requisitos del sistema de gestión ambiental** 4.1 Requisitos generales 4.4 Implementación y operación 4.5.1 Monitoreo y medición
4.3 Requisitos de documentación 4.3.1 Aspectos Generales 4.3.2 Control de documentos 4.3.3 Control de registros	4.2 Requisitos de documentación 4.2.1 Aspectos Generales 4.2.2 Manual de calidad 4.2.3 Control de documentos 4.2.4 Control de registros	4.4.5 Control de la documentación 4.5.4 Control de registros
5 Responsabilidad de la gerencia 5.1 Compromiso de la gerencia	**5 Responsabilidad de la gerencia** 5.1 Compromiso de la gerencia 5.2 Enfoque de los clientes 5.3 Política de calidad 5.4 Planeamiento 5.5 Responsabilidad, autoridad y comunicación	4.2 Política ambiental 4.3 Planeamiento

Norma Peruana	ISO 9001:2000	ISO 14001:2004
5.2 Administración de recursos 5.2.1 Provisión de recursos 5.2.2 Capacitación, concientización y competencia	**6 Gestión de recursos** 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Competencia, concientización y capacitación 6.3 Infraestructura 6.4 Ambiente de trabajo	4.4.2 Competencia, concientización y capacitación
6 Auditorías internas del ISMS	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7 Revisión gerencial del ISMS 7.1 Aspectos Generales 7.2 Revisión: entradas 7.3 Revisión: salidas	**5.6 Revisión gerencial** 5.6.1 Aspectos Generales 5.6.2 Revisión: entradas 5.6.3 Revisión: salidas	**4.6 Revisión gerencial**
8 Mejora del ISMS 8.1 Mejora continua	**8 Mejora** 8.5.1 Mejora continua	
8.2 Acciones correctivas	8.5.3 Acciones correctivas	4.5.3 No conformidad, acciones correctivas y preventivas
8.3 Acciones preventivas	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles **Anexo B Principios OECD y de esta Norma** **Anexo C Correspondencia entre la norma ISO 9001: 2000, ISO 14001:2004 y esta Norma**	**Anexo A Correspondencia entre la norma ISO 9001: 2000, ISO 14001:1996**	**Anexo A Pautas en el uso de esta norma** **Anexo B Correspondencia entre la norma ISO 14001: 2004, ISO 9001:2000**

BIBLIOGRAFÍA

Publicaciones

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 14001:2004, 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