NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

2006-03-22

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS

ICONTEC

E: INFORMATION TECHNOLOGY. SECURITY TECHNIQUES. INFORMATION SECURITY MANAGEMENT SYSTEMS. REQUIREMENTS

CORRESPONDENCIA:	esta norma es una adopción idéntica (IDT) por traducción, respecto a su documento de referencia, la norma ISO/IEC 27001.
DESCRIPTORES:	sistemas de gestión – seguridad de la información; seguridad de la información - requisitos.

I.C.S.: 35.040.00

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. 6078888 - Fax 2221435

Editada 2006-04-03

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La NTC-ISO/IEC 27001 fue ratificada por el Consejo Directivo del 2006-03-22.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 181 Técnicas de seguridad de la información.

AV VILLAS
ASOCIACIÓN BANCARIA DE COLOMBIA
BANCO CAJA SOCIAL/ COLMENA BCSC
BANCO GRANAHORRAR
BANCO DE LA REPÚBLICA
BANISTMO
COLSUBSIDIO
D.S. SISTEMAS LTDA.
ETB S.A. ESP
FLUIDSIGNAL GROUP S.A.
IQ CONSULTORES
IQ OUTSOURCING S.A.
MEGABANCO
NEW NET S.A.
SOCIEDAD COLOMBIANA DE ARCHIVÍSTAS
UNIVERSIDAD NACIONAL DE COLOMBIA

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

ABN AMRO BANK
AGENDA DE CONECTIVIDAD
AGP COLOMBIA
ALPINA S.A.
ASESORÍAS EN SISTEMATIZACIÓN DE DATOS S.A.
ASOCIACIÓN LATINOAMERICANA DE PROFESIONALES DE SEGURIDAD INFORMÁTICA COLOMBIA
ATH
BANCAFÉ
BANCO AGRARIO DE COLOMBIA
BANCO COLPATRIA RED MULTIBANCA COLPATRIA
BANCO DAVIVIENDA
BANCO DE BOGOTÁ
BANCO DE COLOMBIA
BANCO DE CRÉDITO
BANCO DE CRÉDITO HELM FINANCIAL SERVICES
BANCO DE OCCIDENTE
BANCO MERCANTIL DE COLOMBIA
BANCO POPULAR
BANCO SANTANDER COLOMBIA
BANCO STANDARD CHARTERED COLOMBIA
BANCO SUDAMERIS COLOMBIA
BANCO SUPERIOR
BANCO TEQUENDAMA

BANCO UNIÓN COLOMBIANO
BANK BOSTON
BANK OF AMERICA COLOMBIA
BBVA BANCO GANADERO
BFR S.A.
CENTRO DE APOYO A LA TECNOLOGÍA INFORMÁTICA -CATI-
CITIBANK
COINFIN LTDA.
COLGRABAR LTDA.
COMPAÑÍA AGRÍCOLA DE SEGUROS DE VIDA
CONSTRUYECOOP
CORPORACIÓN FINANCIERA COLOMBIANA
CORPORACIÓN FINANCIERA CORFINSURA
CORPORACIÓN FINANCIERA DEL VALLE
CREDIBANCO VISA
CYBERIA S.A.
ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS -EAN-
FEDERACIÓN COLOMBIANA DE LA INDUSTRIA DEL SOFTWARE - FEDESOFT-
DEFENSORÍA DEL CLIENTE FINANCIERO
FINAMÉRICA S. A.
FUNDACIÓN SOCIAL
INCOCRÉDITO
INDUSTRIAS ALIADAS S.A.
INTERBANCO
MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
MINISTERIO DE DEFENSA
N.C.R.
NEXOS SOFTWARE LTDA.
REDEBAN MULTICOLOR
SECRETARÍA DE HACIENDA DISTRITAL
SERVIBANCA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
TMC & CÍA
UNIDAD DE SERVICIOS TECNOLÓGICOS LTDA.
UNIVERSIDAD DE LOS ANDES
UNIVERSIDAD JAVERIANA
WORLDCAD LTDA.

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

Página

Página

0. INTRODUCCIÓN

0.1 GENERALIDADES

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

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

0.2 ENFOQUE BASADO EN PROCESOS

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

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

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

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

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

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

c) el seguimiento y revisión del desempeño y eficacia del SGSI, y

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

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

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

EJEMPLO 1 Un requisito podría ser que las violaciones a la seguridad de la información no causen daño financiero severo a una organización, ni sean motivo de preocupación para ésta.

EJEMPLO 2 Una expectativa podría ser que si ocurre un incidente serio, como por ejemplo el *Hacking* del sitio web de una organización, haya personas con capacitación suficiente en los procedimientos apropiados, para minimizar el impacto.

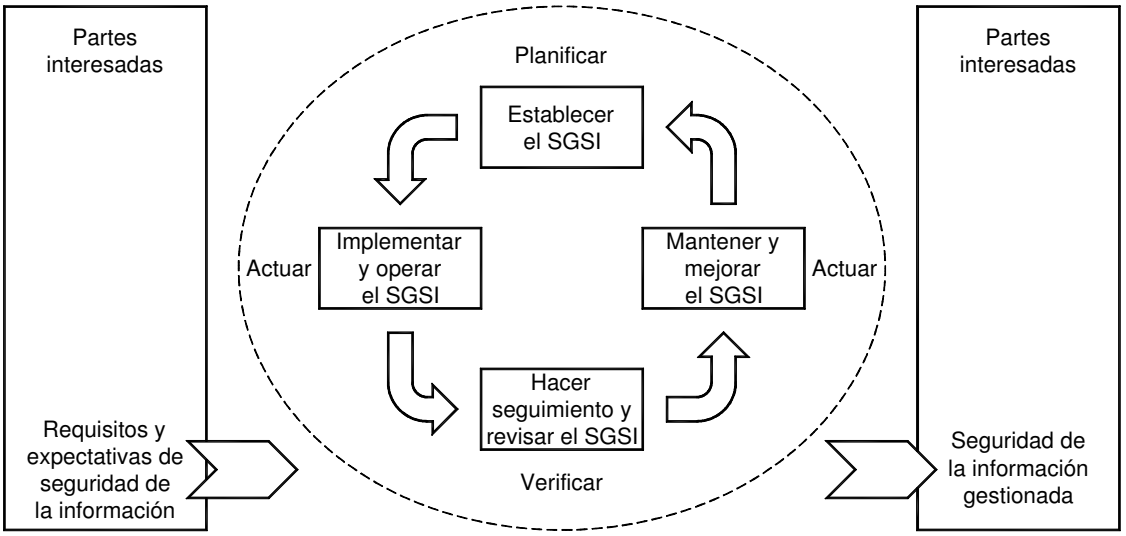

Figura 1. Modelo PHVA aplicado a los procesos de SGSI

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

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

0.3 COMPATIBILIDAD CON OTROS SISTEMAS DE GESTIÓN

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

Esta norma está diseñada para permitir que una organización alinee o integre su SGSI con los requisitos de los sistemas de gestión relacionados.

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS

1. OBJETO

1.1 GENERALIDADES

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

El SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.

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

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

1.2 APLICACIÓN

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

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

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

2. REFERENCIA NORMATIVA

El siguiente documento referenciado es indispensable para la aplicación de esta norma. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento referenciado (incluida cualquier corrección).

NTC-ISO/IEC 17799:2006, Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

3. TÉRMINOS Y DEFINICIONES

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

3.1
aceptación del riesgo
decisión de asumir un riesgo.

[Guía ISO/IEC 73:2002]

3.2.
activo
cualquier cosa que tiene valor para la organización.

[NTC 5411-1:2006]

3.3
análisis de riesgo
uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[Guía ISO/IEC 73:2002]

3.4
confidencialidad
propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[NTC 5411-1:2006]

3.5
declaración de aplicabilidad

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

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

3.6
disponibilidad
propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

[NTC 5411-1:2006]

3.7
evaluación del riesgo
proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

[Guía ISO/IEC 73:2002]

3.8
evento de seguridad de la información
presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

[ISO/IEC TR 18044:2004]

3.9
gestión del riesgo
actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

[Guía ISO/IEC 73:2002]

3.10
incidente de seguridad de la información
un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

[ISO/IEC TR 18044:2004]

3.11
integridad
propiedad de salvaguardar la exactitud y estado completo de los activos.

[NTC 5411-1:2006]

3.12
riesgo residual
nivel restante de riesgo después del tratamiento del riesgo.

[Guía ISO/IEC 73:2002]

3.13
seguridad de la información
preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad.

[NTC-ISO/IEC 17799:2006]

3.14
sistema de gestión de la seguridad de la información
SGSI
parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

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

3.15
tratamiento del riesgo
proceso de selección e implementación de medidas para modificar el riesgo.

[Guía ISO/IEC 73:2002]

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

3.16
valoración del riesgo
proceso global de análisis y evaluación del riesgo.

[Guía ISO/IEC 73:2002]

4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 REQUISITOS GENERALES

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

4.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI

4.2.1 Establecimiento del SGSI

La organización debe:

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

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

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

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

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

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

5) haya sido aprobada por la dirección.

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

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

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

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

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

d) Identificar los riesgos

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

2) identificar las amenazas a estos activos.

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

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

e) Analizar y evaluar los riesgos.

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

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

3) estimar los niveles de los riesgos.

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

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

Las posibles acciones incluyen:

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

1) aplicar los controles apropiados.

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

3) evitar riesgos, y

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

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

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

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

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

NOTA El Anexo A contiene una lista amplia de objetivos de control y controles que comúnmente se han encontrado pertinentes en las organizaciones. Se sugiere a los usuarios de esta norma consultar el Anexo A como punto de partida para la selección de controles, con el fin de asegurarse de que no se pasan por alto opciones de control importantes.

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

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

j) Elaborar una declaración de aplicabilidad.

Se debe elaborar una declaración de aplicabilidad que incluya:

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

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

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

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

4.2.2 Implementación y operación del SGSI

La organización debe:

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

b) implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades;

c) implementar los controles seleccionados en el numeral 4.2.1, literal g) para cumplir los objetivos de control;

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

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

e) implementar programas de formación y de toma de conciencia, (véase el numeral 5.2.2);

f) gestionar la operación del SGSI;

g) gestionar los recursos del SGSI (véase el numeral 5.2);

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

4.2.3 Seguimiento y revisión del SGSI

La organización debe:

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

1) detectar rápidamente errores en los resultados del procesamiento;

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

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

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

5) determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

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

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

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

1) la organización,

2) la tecnología,

3) los objetivos y procesos del negocio,

1) las amenazas identificadas,

2) la eficacia de los controles implementados, y

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

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

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

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

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

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

4.2.4 Mantenimiento y mejora del SGSI

La organización debe, regularmente:

a) Implementar las mejoras identificadas en el SGSI;

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

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

d) Asegurar que las mejoras logran los objetivos previstos.

4.3 REQUISITOS DE DOCUMENTACIÓN

4.3.1 Generalidades

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

Es importante estar en capacidad de demostrar la relación entre los controles seleccionados y los resultados del proceso de valoración y tratamiento de riesgos, y seguidamente, con la política y objetivos del SGSI.

La documentación del SGSI debe incluir:

a) declaraciones documentadas de la política y objetivos del SGSI (véase el numeral 4.2.1, literal b));

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

c) los procedimientos y controles que apoyan el SGSI;

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

e) el informe de valoración de riesgos (véase el numeral 4.2.1, literales c) a g));

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

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

h) Los registros exigidos por esta norma (véase el numeral 4.3.3), y

i) La declaración de aplicabilidad.

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

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

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

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

4.3.2 Control de documentos

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

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

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

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

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

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

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

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

h) asegurar que la distribución de documentos esté controlada;

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

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

4.3.3 Control de registros

Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros deben estar protegidos y controlados. El SGSI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros se deben documentar e implementar.

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

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

5. RESPONSABILIDAD DE LA DIRECCIÓN

5.1 COMPROMISO DE LA DIRECCIÓN

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

a) mediante el establecimiento de una política del SGSI;

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

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

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

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

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

g) asegurando que se realizan auditorías internas del SGSI (véase el numeral 6), y

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

5.2 GESTIÓN DE RECURSOS

5.2.1 Provisión de recursos

La organización debe determinar y suministrar los recursos necesarios para:

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

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

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

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

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

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

5.2.2 Formación, toma de conciencia y competencia

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

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

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

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

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

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

6. AUDITORIAS INTERNAS DEL SGSI

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

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

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

c) están implementados y se mantienen eficazmente, y

d) tienen un desempeño acorde con lo esperado.

Se debe planificar un programa de auditorías tomando en cuenta el estado e importancia de los procesos y las áreas que se van a auditar, así como los resultados de las auditorías previas. Se deben definir los criterios, el alcance, la frecuencia y los métodos de la auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

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

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

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

7. REVISIÓN DEL SGSI POR LA DIRECCIÓN

7.1 GENERALIDADES

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

7.2 INFORMACIÓN PARA LA REVISIÓN

Las entradas para la revisión por la dirección deben incluir:

a) resultados de las auditorías y revisiones del SGSI;

b) retroalimentación de las partes interesadas;

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

d) estado de las acciones correctivas y preventivas;

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

f) resultados de las mediciones de eficacia;

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

h) cualquier cambio que pueda afectar el SGSI; y

i) recomendaciones para mejoras.

7.3 RESULTADOS DE LA REVISIÓN

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

a) la mejora de la eficacia del SGSI;

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

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

1) los requisitos del negocio,

2) los requisitos de seguridad,

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

4) los requisitos reglamentarios o legales,

5) las obligaciones contractuales, y

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

d) los recursos necesarios.

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

8. MEJORA DEL SGSI

8.1 MEJORA CONTINUA

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

8.2 ACCIÓN CORRECTIVA

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

a) identificar las no conformidades;

b) determinar las causas de las no conformidades;

c) evaluar la necesidad de acciones que aseguren que las no conformidades no vuelven a ocurrir;

d) determinar e implementar la acción correctiva necesaria;

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

f) revisar la acción correctiva tomada.

8.3 ACCIÓN PREVENTIVA

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

a) identificar no conformidades potenciales y sus causas;

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

c) determinar e implementar la acción preventiva necesaria;

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

e) revisar la acción preventiva tomada.

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

La prioridad de las acciones preventivas se debe determinar con base en los resultados de la valoración de los riesgos.

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

ANEXO A
(Normativo)

OBJETIVOS DE CONTROL Y CONTROLES

A.1 INTRODUCCIÓN

Los objetivos de control y los controles enumerados en la Tabla A.1 se han obtenido directamente de los de la NTC-ISO/IEC 17799:2005, numerales 5 a 15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas se deben seleccionar como parte del proceso de SGSI especificado en el numeral 4.2.1.

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

Tabla A.1. Objetivos de control y controles

A.5 POLÍTICA DE SEGURIDAD			
A.5.1 Política de seguridad de la información Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.			
A.5.1.1	Documento de la política de seguridad de la información.	Control La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	
A.5.1.2	Revisión de la política de seguridad de la información.	Control La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización interna Objetivo: gestionar la seguridad de la información dentro de la organización.			
A.6.1.1	Compromiso de la dirección con la seguridad de la información.	La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.	
A.6.1.2	Coordinación de la seguridad de la información.	Control Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.	
A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	Control Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.	

Continúa . . .

Tabla A.1. (Continuación)

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Control Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.	
A.6.1.5	Acuerdos sobre confidencialidad	Control Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	
A.6.1.6	Contacto con las autoridades	Control Se deben mantener contactos apropiados con las autoridades pertinentes.	
A.6.1.7	Contacto con grupos de interés especiales	Control Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	
A.6.1.8	Revisión independiente de la seguridad de la información.	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.	
A.6.2 Partes externas Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.			
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Control Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.	
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Control Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización	
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Control Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad	

Tabla A.1. (Continuación)

A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad por los activos Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.		
A.7.1.1	Inventario de activos	Control Todos los activos deben estar claramente identificados y se deben 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 servicios 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 identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información
A.7.2 Clasificación de la información Objetivo: asegurar que la información recibe el nivel de protección adecuado.		
A.7.2.1	Directrices de clasificación	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
A.7.2.2	Etiquetado y manejo de información	Control Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.1 Antes de la contratación laboral [4)] Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.			
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	

3) El término "propietario" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

4) Explicación: La palabra “contratación laboral" cubre todas las siguientes situaciones: empleo de personas (temporal o a término indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos acuerdos

Tabla A.1. (Continuación)

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.1.2	Selección	Control Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos	
A.8.1.3	Términos y condiciones laborales.	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	
A.8.2 Durante la vigencia de la contratación laboral Objetivo*:* asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.			
A.8.2.1	Responsabilidades de la dirección	Control La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	

Tabla A.1. (Continuación)

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.3 Terminación o cambio del contratación laboral Objetivo: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada..			
A.8.3.1	Responsabilidades en la terminación	Control Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	
A.8.3.3	Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.1 Áreas seguras Objetivo*:* evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.			
A.9.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	
A.9.1.2	Controles de acceso físico.	Control Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Control Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	
A.9.1.4	Protección contra amenazas externas y ambientales.	Control Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	
A.9.1.5	Trabajo en áreas seguras.	Control Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.	

Tabla A.1. (Continuación)

A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.2 Seguridad de los equipos Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.			
A.9.2.1	Ubicación y protección de los equipos.	Control Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	
A.9.2.2	Servicios de suministro	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	
A.9.2.3	Seguridad del cableado.	Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.	
A.9.2.4	Mantenimiento de los equipos.	Control Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	Control Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos.	Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	
A.9.2.7	Retiro de activos	Control Ningún equipo, información ni software se deben retirar sin autorización previa.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1 Procedimientos operacionales y responsabilidades Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.			
A.10.1.1	Documentación de los procedimientos de operación	Control Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	
A.10.1.2	Gestión del cambio.	Control Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.	

Tabla A.1. (Continuación)

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1.3	Distribución de funciones.	Control Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Control Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	
A.10.2 Gestión de la prestación del servicio por terceras partes Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.			
A.10.2.1	Prestación del servicio	Control Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Control Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Control Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	
A.10.3 Planificación y aceptación del sistema Objetivo*:* minimizar el riesgo de fallas de los sistemas.			
A.10.3.1	Gestión de la capacidad.	Control Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	
A.10.3.2	Aceptación del sistema.	Control Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	

Tabla A.1. (Continuación)

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.4 Protección contra códigos maliciosos y móviles Objetivo: proteger la integridad del software y de la información.			
A.10.4.1	Controles contra códigos maliciosos.	Control Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	
A.10.5 Respaldo Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de linformación.			
A.10.5.1	Respaldo de la información.	Control Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	
A.10.6 Gestión de la seguridad de las redes Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.			
A.10.6.1	Controles de las redes.	Control Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	
A.10.6.2	Seguridad de los servicios de la red.	Control En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.	
A.10.7 Manejo de los medios Objetivo*:* evitar la divulgación , modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.			
A.10.7.1	Gestión de los medios removibles	Control Se deben establecer procedimientos para la gestión de los medios removibles	
A.10.7.2	Eliminación de los medios.	Control Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.	

Tabla A.1. (Continuación)

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.7.3	Procedimientos para el manejo de la información.	Control Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	
A.10.7.4	Seguridad de la documentación del sistema.	Control La documentación del sistema debe estar protegida contra el acceso no autorizado.	
A.10.8 Intercambio de la información Objetivo*:* mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.			
A.10.8.1	Políticas y procedimientos para el intercambio de información	Control Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	
A.10.8.2	Acuerdos para el intercambio	Control Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.	
A.10.8.3	Medios físicos en tránsito.	Control Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	
A.10.8.4	Mensajería electrónica.	Control La información contenida en la mensajería electrónica debe tener la protección adecuada	
A.10.8.5	Sistemas de información del negocio.	Control Se deben establecer, 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: garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.			
A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración , divulgación , duplicación o repetición no autorizada del mensaje.	

Tabla A.1. (Continuación)

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.9.3	Información disponible al público	Control La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	
A.10.10 Monitoreo Objetivo: detectar actividades de procesamiento de la información no autorizadas.			
A.10.10.1	Registro de auditorías	Control Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	
A.10.10.2	Monitoreo del uso del sistema	Control Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	
A.10.10.3	Protección de la información del registro	Control Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	
A.10.10.4	Registros del administrador y del operador	Control Se deben registrar las actividades tanto del operador como del administrador del sistema..	
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	
A.10.10.6	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	
A.11 CONTROL DE ACCESO			
A.11.1 Requisito del negocio para el control de acceso Objetivo: controlar el 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 con base en los requisitos del negocio y de la seguridad para el acceso	
A.11.2 Gestión del acceso de usuarios Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.			

Tabla A.1. (Continuación)

A.11 CONTROL DE ACCESO			
A.11.2.1	Registro de usuarios.	Control Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el 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 privilegios.	
A.11.2.3	Gestión de contraseñas para usuarios.	Control La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	Control La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	
A.11.3 Responsabilidades de los usuarios Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.			
A.11.3.1	Uso de contraseñas.	Control Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	
A.11.3.2	Equipo de usuario desatendido.	Control Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	
A.11.3.3	Política de escritorio despejado y de pantalla despejada	Control Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	
A.11.4 Control de acceso a las redes Objetivo: evitar el acceso no autorizado a servicios en red.			
A.11.4.1	Política de uso de los servicios de red.	Control Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	
A.11.4.2	Autenticación de usuarios para conexiones externas.	Control Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	
A.11.4.3	Identificación de los equipos en las redes.	Control La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	

Tabla A.1. (Continuación)

A.11 CONTROL DE ACCESO			
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	Control El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado	
A.11.4.5	Separación en las redes.	Control En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	
A.11.4.6	Control de conexión a las redes.	Control Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).	
A.11.4.7	Control de enrutamiento en la red.	Control Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	
A.11.5 Control de acceso al sistema operativo			
Objetivo: evitar el acceso no autorizado a los sistemas operativos.			
A.11.5.1	Procedimientos de ingreso seguros	Control El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	
A.11.5.2	Identificación y autenticación de usuarios.	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	
A.11.5.3	Sistema de gestión de contraseñas.	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	
A.11.5.4	Uso de las utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	
A.11.5.5	Tiempo de inactividad de la sesión	Control Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.	
A.11.5.6	Limitación del tiempo de conexión.	Control Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	

Tabla A.1. (Continuación)

A.11 CONTROL DE ACCESO			
A.11.6 Control de acceso a las aplicaciones y a la información Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.			
A.11.6.1	Restricción de acceso a la información.	Control Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	
A.11.6.2	Aislamiento de sistemas sensibles.	Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	
A.11.7 Computación móvil y trabajo remoto Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.			
A.11.7.1	Computación y comunicaciones móviles.	Control Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	
A.11.7.2	Trabajo remoto.	Control Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.1 Requisitos de seguridad de los sistemas de información Objetivo*:* garantizar que la seguridad es parte integral de los sistemas de información.			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.			
A.12.2.1	Validación de los datos de entrada.	Control Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	
A.12.2.2	Control de procesamiento interno.	Control Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	

Tabla A.1. (Continuación)

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.2.3	Integridad del mensaje.	Control Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	
A.12.2.4	Validación de los datos de salida.	Control Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias	
A.12.3 Controles criptográficos Objetivo*:* proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.			
A.12.3.1	Política sobre el uso de controles criptográficos.	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	
A.12.3.2	Gestión de llaves.	Control Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	
A.12.4 Seguridad de los archivos del sistema Objetivo: garantizar la seguridad de los archivos del sistema.			
A.12.4.1	Control del software operativo.	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	
A.12.4.2	Protección de los datos de prueba del sistema.	Control Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse	
A.12.4.3	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.	
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.			
A.12.5.1	Procedimientos de control de cambios.	Control Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	

Tabla A.1. (Continuación)

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Control Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	
A.12.5.4	Fuga de información	Control Se deben evitar las oportunidades para que se produzca fuga de información.	
A.12.5.5	Desarrollo de software contratado externamente	Control La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.			
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN			
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.			
A.13.1.1	Reporte sobre los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	
A.13.1.2	Reporte sobre las debilidades de la seguridad	Control Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.			
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Control Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	

Tabla A.1. (Continuación)

A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.13.2.3	Recolección de evidencia	Control Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.			
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	
A.14.1.2	continuidad del negocio y evaluación de riesgos	Control Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.	
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Control Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Control Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	

Tabla A.1. (Continuación)

A.15 CUMPLIMIENTO			
A.15.1 Cumplimiento de los requisitos legales Objetivo*:* evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.			
A.15.1.1	Identificación de la legislación aplicable.	Control Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización	
A.15.1.2	Derechos de propiedad intelectual (DPI).	Control Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	
A.1.5.1.3	Protección de los registros de la organización.	Control Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	
A.15.1.4	Protección de los datos y privacidad de la información personal.	Control Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Control Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	
A.15.1.6	Reglamentación de los controles criptográficos.	Control Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico Objetivo*:* asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización..			
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	Control Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.	
A.15.2.2	Verificación del cumplimiento técnico.	Control Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	

Tabla A.1. (Final)

A.15 CUMPLIMIENTO			
A.15.3 Consideraciones de la auditoría de los sistemas de información Objetivo*:* maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.			
A.15.3.1	Controles de auditoría de los sistemas de información.	Control Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Control Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.	

ANEXO B
(Informativo)

PRINCIPIOS DE LA OCDE Y DE ESTA NORMA

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

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

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

ANEXO C
(Informativo)

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

La Tabla C.1 muestra la correspondencia entre la NTC ISO 9001:2000, la NTC-ISO 14001:2004 y la presente norma internacional.

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

Esta norma	NTC- ISO 9001:2000	NTC- ISO 14001:2004
0.Introducción 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Compatibilidad con otros sistemas de gestión	0. Introducción 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Relación con la norma ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	Introducción
1 Objeto 1.1 Generalidades 1.2 Aplicación	1. Objeto y campo de aplicación 1.1 Generalidades 1.2 Aplicación	1. Objeto y campo de aplicación
2 Referencia normativa	2. Referencias normativas	2. Referencias normativas
3 Términos y definiciones	3. Términos y definiciones	3. Términos y definiciones
4. Sistema de gestión de la seguridad de la información 4.1 Requisitos generales 4.2 Establecimiento y gestión del SGSI 4.2.1 Establecimiento del SGSI 4.2.2 Implementación y operación del SGSI 4.2.3 Seguimiento y revisión del SGSI	4. Sistema de gestión de la calidad 4.1 Requisitos generales 8.2.3 Seguimiento y medición de los procesos 8.2.4 Seguimiento y medición del producto	4. Requisitos del sistema de gestión ambiental 4.1 Requisitos generales 4.4 Implementación y operación 4.5.1 Seguimiento y medición
4.2.4 Mantenimiento y mejora del SGSI		

Continúa . . .

Tabla C.1. (Final)

Esta norma	NTC- ISO 9001:2000	NTC- ISO 14001:2004
4.3 Requisitos de documentación 4.3.1 Generalidades 4.3.2 Control de documentos 4.3.3 Control de registros	4.2 Requisitos de la documentación 4.2.1 Generalidades 4.2.2 Manual de la calidad 4.2.3 Control de los documentos 4.2.4 Control de los registros	 4.4.5 Control de documentos 4.5.4 Control de los registros
5. Responsabilidad de la dirección 5.1 Compromiso de la dirección	5. Responsabilidad de la dirección 5.1 Compromiso de la dirección 5.2 Enfoque al cliente 5.3 Política de la calidad 5.4 Planificación 5.5 Responsabilidad, autoridad y comunicación	 4.2 Política ambiental 4.3 Planificación
5.2 Gestión de recursos 5.2.1 Provisión de recursos 5.2.2 Formación, toma de conciencia y competencia	6. Gestión de los recursos 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Competencia, toma de conciencia y formación 6.3 Infraestructura 6.4 Ambiente de trabajo	 4.4.2 Competencia, formación y toma de conciencia
6. Auditorías internas del SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7. Revisión del SGSI por la dirección 7.1 Generalidades 7.2 Información para la revisión 7.3 Resultados de la revisión	5.6 Revisión por la dirección 5.6.1 Generalidades 5.6.2 Información para la revisión 5.6.3 Resultados de la revisión	4.6 Revisión por la dirección
8. Mejora del SGSI 8.1 Mejora continua	8.5 Mejora 8.5.1 Mejora continua	
8.2 Acción correctiva	8.5.2 Acciones correctivas	4.5.3 No conformidad, acción correctiva y acción preventiva
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles Anexo B Principios de la OCDE y de esta norma Anexo C Correspondencia entre la NTC-ISO 9001:2000, la NTC-ISO 14001:2004 y la presente norma	 Anexo A Correspondencia entre las normas ISO 9001:2000 y la ISO 14001:1996	Anexo A Orientación para el uso de esta norma internacional Anexo B Correspondencia entre la ISO 14001:2004 y la ISO 9001:2000

BIBLIOGRAFÍA

[1] NTC-ISO 9001:2000, Sistemas de gestión de la calidad. Requisitos.

[2] NTC-ISO 14001:2004, Sistemas de gestión ambiental. Requisitos con orientación para su uso.

[3] NTC-ISO 19011:2002, Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiente.

[4] GTC 36 Requisitos generales para organismos que realizan evaluación y certificación/registro de sistemas de calidad. (ISO/IEC Guide 62)

[5] NTC 5411-1 Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones (ISO/IEC 13335-1:2004).

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

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

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

[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 Engineerig Study, 1986.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva, ISO. pp 34 (ISO/IEC 27001: 2005)