NORMA ARGENTINA

IRAM-ISO/IEC 27001

Primera edición
2007-12-28

Tecnología de la información

Sistemas de gestión de la seguridad de la información (SGSI)

Requisitos

Information technology
Information security management systems
Requirements

* **La presente reemplaza a la norma IRAM 17798: 2004.**

Referencia Numérica:
IRAM-ISO/IEC 27001:2007

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor .

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

Esta norma es una adopción idéntica de la norma ISO/IEC 27001:2005.

La presente reemplaza a la norma IRAM 17798: 2004.

Prefacio ISO

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

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

La tarea principal del comité técnico conjunto es la de preparar normas internacionales. Los proyectos de normas internacionales adoptadas por el comité técnico conjunto son circulados a los organismos nacionales y sometidos a votación. La publicación como Norma Internacional requiere la aprobación de al menos el 75% de los organismos nacionales.

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

La norma ISO/IEC 27001 fue preparada por el comité técnico conjunto ISO/IEC JTC1, *Tecnología de la Información*, subcomité SC 27, *Técnicas de seguridad en TI.*

Índice

Tecnología de la información

Sistemas de gestión de la seguridad de la información (SGSI)

Requisitos

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). Se recomienda que la adopción de un SGSI sea una decisión estratégica para una organización. El diseño e implementación de un SGSI de una organización se ve influenciado por sus 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 esté de acuerdo con la escala de necesidades de la organización, por ejemplo: una situación simple requiere una solución de SGSI simple.

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

0.2 ENFOQUE BASADO EN PROCESOS

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

Para funcionar eficazmente, una organización necesita identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que emplee 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 de estos procesos, y su gestión, pueden ser denominadas 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 poner énfasis en la importancia de:

a) comprender los requisitos de seguridad de la información de una organización, y la necesidad de establecer la pol ítica y objetivos en relación con la seguridad de la información;

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

c) el seguimiento y revisión del desempeño y efectividad 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 y expectativas de seguridad de la información de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. La figura 1 también ilustra los vínculos en los procesos especificados en los capítulos 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 sólido para implementar los principios en aquellas directrices que gobiernan la evaluación de riesgos, el diseño e implementación de la seguridad, la gestión y reevaluación de la seguridad.

EJEMPLO 1

Un requisito podría ser que las violaciones a la seguridad de la información no causen daños financieros serios a una organización y no le causen descrédito.

EJEMPLO 2

Una expectativa podría ser que si ocurre un incidente serio (por ejemplo: el *hacking* del sitio en Internet de comercio electrónico de una organización) es conveniente que haya personas con capacitación suficiente en los procedimientos apropiados para minimizar el impacto.

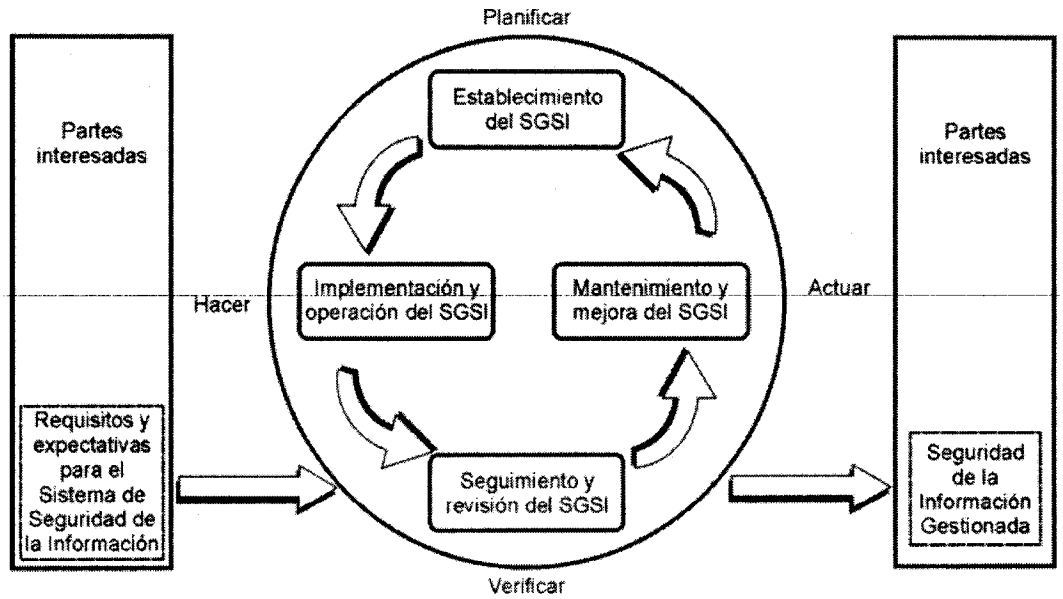

Figura 1 – Modelo PHVA aplicado a los procesos del SGSI

Planificar (establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos del SGSI 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 organi zación.
Hacer (implementar y operar el SGSI)	Implementar y poner en pr áctica la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer el seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempe fio del proceso contra la política y los objetivos de seguridad y la e xperiencia práctica del SGSI, e informar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y pr eventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección u otra información correspondiente, para lograr la mejora continua del SGSI.

[1] OECD Guidelines for de Security of Information System and Networks – Towards a Culture of Security. Paris: OECD, Julio 2002.

0.3 COMPATIBILIDAD CON OTROS SISTEMAS DE GESTIÓN

Esta norma está alineada con la IRAM-ISO 9001: 2000 y la IRAM-ISO 14001:2005, con el fin de apoyar la implementación y operación, consistente e integrada 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 capítulos de esta norma, la IRAM-ISO 9001:2000 y la IRAM-ISO 14001:2005.

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

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

1 OBJETO

1.1 GENERALIDADES

Esta norma alcanza a todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos de negocio globales 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 adecuados y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.

NOTA 1. Se recomienda que las referencias que se hacen en esta norma a *negocio* se interpreten ampliamente como aquellas actividades que son esenciales para la existencia de la organización.

NOTA 2. La IRAM-ISO/IEC 27002 brinda orientación sobre la implementación, que se puede usar cuando se diseñan controles.

NOTA IRAM 1. Esta norma está aún en estudio a nivel IRAM.

1.2 APLICACIÓN

Los requisitos establecidos en esta norma son genéricos y la intención es que sean aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requisitos especificados en los capítulos 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 estar justificada y es necesario que se suministre evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables. Cuando 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 o su responsabilidad para ofrecer la seguridad de la información que satisfaga los requisitos de seguridad determinados por la evaluación de riesgos y las leyes aplicables o los requisitos reglamentarios.

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

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Los documentos normativos que se indican a continuación son indispensables para la aplicación de este documento.

Para los documentos normativos en los que se indica el año de publicación, se aplican las ediciones citadas.

Para los documentos normativos en los que no se indica el año de publicación, se aplican las ediciones vigentes, incluyendo todas sus modificaciones.

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

NOTA IRAM 2. Actualmente esta norma pasó a ser ISO/IEC 27002 y está en estudio a nivel IRAM como IRAM-ISO/IEC 27002 *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 términos y definiciones siguientes:

NOTA IRAM 3. La numeración entre paréntesis es la obrante en la ISO/IEC 27001:2005.

3.1 (3.10)
aceptación del riesgo
decisión de asumir un riesgo.

[Guía ISO/IEC 73:2002]

3.2 (3.1)
activo
cualquier cosa que tenga valor para la organización.

[ISO/IEC 13335-1:2004]

3.3 (3.11)
análisis de riesgo
uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[Guía ISO/IEC 73:2002]

3.4 (3.3)
confidencialidad
propiedad que determina que la información no esté disponible ni puede ser revelada a individuos, entidades o procesos no autorizados.

[ISO/IEC 13335-1:2004]

3.5 (3.16)
declaración de aplicabilidad
declaración documentada que describe los objetivos de control y los controles pertinentes y aplicables al SGSI de la organización.

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

3.6 (3.2)
disponibilidad
propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.

[ISO/IEC 13335-1:2004]

3.7 (3.12)
evaluación del riesgo
proceso global de análisis de riesgo y valoración del riesgo.

[Guía ISO/IEC 73:2002]

3.8 (3.5)
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 (3.14)
gestión del riesgo
actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

[Guía ISO/IEC 73:2002]

3.10 (3.6)
incidente de seguridad de la información.
un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

[ISO/IEC TR 18044:2004]

3.11 (3.8)
integridad
propiedad de salvaguardar la exactitud y estado completo de los activos.

[ISO/IEC 13335-1:2004]

3.12 (3.9)
riesgo residual
nivel restante de riesgo después del tratamiento del riesgo.

[Guía ISO/IEC 73:2002]

3.13 (3.4)
seguridad de la información
preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar ("accountability"), no repudio y fiabilidad.

[ISO/IEC 17799:2005]

3.14 (3.7)
sistema de gestión de la seguridad de la información
SGSI
parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

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

3.15 (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 (3.13)
valoración del riesgo
proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

[Guía ISO/IEC 73:2002]

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, dentro del contexto de las actividades globales de la organización y de los riesgos que enfrenta. Para los propósitos de esta norma, el proceso utilizado 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 hacer lo siguiente:

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

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

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

   2) tenga en cuenta los requisitos de la actividad de la organización, legales o reglamentarios, y las obligaciones de seguridad contractuales;

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

   4) establezca los criterios contra los cuales se evaluará el riesgo. (ver 4.2.1c)); y

5) haya sido aprobada por la dirección.

NOTA. Para los propósitos de esta norma, la política del SGSI se considera como un gran conjunto de políticas de seguridad de la in formación. Estas políticas pueden estar descriptas en un solo documento.

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

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

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

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

NOTA. Existen diferentes metodologías para la evaluación de riesgos. Ejemplos de Metodologías de evaluación de riesgos se discuten en la ISO/IEC TR 13335-3, *Information technology. Guidelines for the Management of IT Security – Techniques for the Management of IT Security.*

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 pueda tener sobre estos activos.

e) Analizar y evaluar los riesgos.

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

2) Evaluar la posibilidad real de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades y los impactos asociados con estos activos, así como también los controles implementados hasta el momento.

3) Estimar los niveles de los riesgos.

4) Determinar si se acepta el riesgo o si es necesario su tratamiento a partir de los criterios establecidos en 4.2.1 c) 2).

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

Las posibles acciones incluyen :

1) aplicar los controles apropiados ;

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

3) evitar riesgos; y

4) transferir a otras partes los riesgos de la actividad de la organización asociados, por ejemplo: a aseguradoras, proveedores, etc.

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

Se deben seleccionar e implementar los objetivos de control y los controles de manera que cumplan con los requisitos identificados en el proceso de evaluación de riesgos y tratamiento de riesgos. Esta selección debe tener en cuenta los criterios para la aceptación de riesgos (ver 4.2.1 c) 2)), al igual que los requisitos legales, reglamentarios y contractuales.

[2] El término *propietario* identifica a un individuo o entidad que tiene responsabilidad aprobada por la alta dirección de controlar la producción, de sarrollo, mantenimiento, uso y seguridad de los activos. El término *propietario* no se refiere a que la persona real mente tiene derecho alguno de propiedad sobre el activo.

Los objetivos de control y los controles del anexo A deben ser seleccionados como parte de este proceso, en tanto sean adecuados para cubrir los requisitos identificados.

Los objetivos de control y los controles presentados en el anexo A no son exhaustivos, por lo que se pueden seleccionar objetivos de control y controles adicionales.

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

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

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

j) Elaborar una declaración de aplicabilidad.

Se debe elaborar una Declaración de Aplicabilidad que incluya lo siguiente :

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

2) los objetivos de control y los controles implementados corrientemente (ver 4.2.1 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 verificar que ningún control se haya omitido involuntariamente.

4.2.2 Implementación y operación del SGSI

La organización debe realizar lo siguiente:

a) formular un plan para el tratamiento de los riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para gestionar los riesgos de seguridad de la información (ver cap ítulo 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 4.2.1 g) para cumplir los objetivos de control;

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

NOTA. La medición de la eficacia de los controles permite a la alta dirección 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, (ver 5.2.2);

f) gestionar la operación del SGSI;

g) gestionar los recursos del SGSI (ver 5.2);

h) implementar procedimientos y otros controles para detectar y dar rápida respuesta a los incidentes de seguridad (ver 4.2.3).

4.2.3 Seguimiento y revisión del SGSI

La organización debe realizar lo siguiente:

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

1) detectar rápidamente errores en los resultados del procesamiento;

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

3) posibilitar que la alta 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 auditorías de seguridad, incidentes, resultados de las mediciones de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.

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

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

1) la organización;

2) la tecnología;

3) los objetivos y procesos del negocio;

4) las amenazas identificadas;

5) la eficacia de los controles implementados; y

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

e) Realizar auditorías internas del SGSI a intervalos planificados (ver 6).

NOTA. Las auditorías internas, denominadas algunas veces auditorías de primera parte, las realiza la propia organización u otra organización en su nombre, para fines 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 han identificado mejoras en el proceso de SGSI (ver 7.1).

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

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

4.2.4 Mantenimiento y mejora del SGSI

La organización debe, regularmente, hacer lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

b) Emprender las acciones correctivas y preventivas adecuadas de acuerdo con 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 alta dirección, 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 evaluación y tratamiento de riesgos, y seguidamente, con la política y objetivos del SGSI.

La documentación del SGSI debe incluir:

a) declaraciones documentadas de la política (ver 4.2.1 b)) y objetivos del SGSI;

b) el alcance del SGSI (ver 4.2.1 a));

c) los procedimientos y controles que apoyan el SGSI;

d) una descripción de la metodolo gía de evaluación de riesgos (ver 4.2.1 c));

e) el informe de evaluación de riesgos (ver 4.2.1 c) a g));

f) el plan de tratamiento de riesgos (ver 4.2.2 b));

g) los procedimientos documentados que necesita la organización para asegurar la planificación, operación y control eficaz de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles (ver 4.2. 3 c));

h) los registros exigidos por esta norma (ver 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, implem entado y mantenido.

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

- la dimensión de la organización y el tipo de sus acti vidades, y
- el alcance y complejidad de los requisitos de seguridad y del sistema que se está administrando.

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

4.3.2 Control de documentos

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

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

b) revisar y actualizar los documentos seg ún sea necesario y reaprobarlos;

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

d) asegurar que las versiones m ás 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 re gistros

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. Se deben documentar e implementar los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros.

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

EJEMPLO - Algunos ejemplos de registros son: un libro de visitantes, informes de auditorías y formularios 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 legales y la necesidad de la mejora continua;

e) brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI (ver 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 (ver 6); y

h) efectuando las revisiones por la dirección, del SGSI (ver 7).

5.2 GESTIÓN DE LOS RECURSOS

5.2.1 Provisión de los 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 adecuada mediante la aplicación correcta de todos los controles implementados;

e) llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente frente 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 (ver 4.3.3).

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

6 AUDITORÍAS INTERNAS DEL SGSI

La organización debe llevar a cabo auditor ías 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 (ver 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 demoras injustificadas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de la verificación.

NOTA. La IRAM-ISO 19011:2005, 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 S GSI.

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, y también la política de seguridad y los objetivos de seguridad. Se deben documentar claramente los resultados de las revisiones y se deben llevar registros de ellos (ver 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 en:

   1) los requerimientos de la actividad,

   2) los requisitos de seguridad,

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

   4) los requisitos reglamentarios o legales,

   5) las obligaciones contractuales, y

   6) los niveles de riesgo y los criterios de aceptación de riesgos;

d) los recursos necesarios;

e) la mejora del método de medición de 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 alta 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 (ver 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, para prevenir su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir requisitos para:

a) identificar no conformidades potenciales y sus causas;

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

c) determinar e implementar la acción preventiva necesaria;

d) registrar los resultados de la acción tomada (ver 4.3.3); y

e) revisar la acción preventiva tomada.

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

Se deben determinar la prioridad de las acciones preventivas en base a los resultados de la evaluación 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

Los objetivos de control y controles indicados en la tabla A.1 están directamente derivados y alineados con aquellos indicados en la IRAM-ISO/IEC 27002, C apítulos 5 al 15. Los listados en la tabla A.1 no son exhaustivos y una organización puede considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas deben ser seleccionados como parte del proceso de S GSI especificado en 4.2.1.

IRAM-ISO/IEC 27002, Capítulos 5 al 15 provee consejos y guías de las mejores prácticas de implementación para sustentar los controles especificados en A.5 a A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad		
A.5.1 Política de seguridad de la información Objetivo: Proporcionar la dirección y el apoyo de la alta dirección para la seguridad de la información, de acuerdo con los requerimientos del negocio y las leyes y regulaciones correspondientes.		
A.5.1.1	Documentación de la política de seguridad de la información	Control Los responsables de la alta dirección deben aprobar un documento que contenga la política de seguridad de la información, publicarlo y comunicarlo a todos los empleados y a terceras partes relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe revisarse a intervalos planificados, o si ocurren cambios significativos para asegurar que continúa siendo conveniente, adecuada y efectiva.
A.6 Organización de la seguridad		
A.6.1 Organización interna Objetivo: Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso gerencial hacia la seguridad de la información	Control La dirección debe dar soporte activo a la seguridad dentro de la organización a través de una directiva clara, compromiso demostrado, asignación explícita, y conocimientos de responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	Control Las actividades de seguridad de la información deben estar coordinadas por representantes de diferentes partes de la organización con los roles y funciones de trabajo correspondientes.
A.6.1.3	Asignación de responsabilidades en materia de seguridad de la información	Control Se deben definir claramente todas las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para las instalaciones de procesamiento de información	Control Se debe establecer e implementar un proceso para autorizar nuevas instalaciones de procesamiento de la información.
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar perió dicamente los requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de protección de la información de la organización.

(Continúa)

Tabla A.1 (continuación)

A.6.1.6	Contacto con autoridades	Control Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener los contactos adecuados con grupos de interés especial u otras asociaciones de pro fesionales y foros de especialistas en seguridad.
A.6.1.8	Revisión independiente de seguridad de la información	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (por ejemplo: objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado en forma independiente a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad.
A.6.2 Partes externas Objetivo: Mantener la seguridad de la información de la or ganización y las instalaciones de procesamiento de información que son accedidas, procesadas, comunicadas o gestionadas por partes e xternas.		
A.6.2.1	Identificación de riesgos relacionados con las partes externas	Control Se deben identificar los riesgos para la información de la organización y para las instalaciones de procesamiento de la información de los procesos de negocios que involucren partes externas, y se deben implementar los controles apropiados antes de conceder el acceso.
A.6.2.2	Asignación de seguridad cuando se trata con clientes	Control Se deben aclarar todos los requer imientos de seguridad identificados antes de otorgarle a los clientes el acceso a la información o a los activos de la organización.
A.6.2.3	Asignación de la seguridad en acuerdos con terceras partes	Control Los acuerdos con terceras partes que involucren el acceso, procesamiento, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de la información, o el agregado de productos o servicios a las instalaciones de procesamiento de información, deben cubrir todos los requerimientos de seguridad importantes.
A.7 Gestión de activos		
A.7.1 Responsabilidad por los activos Objetivo: Alcanzar y mantener una adecuada protección de los activos de la organización.		
A.7.1.1	Inventario de los activos	Control Se deben identificar claramente todos los activos, elaborando y manteniendo un inventario de los activos m ás importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con las instalaciones de procesamiento de la información deben ser propiedad [3] de una parte de la organización designada para ello.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

(Continúa)

[3] El término *propietario* identifica a un individuo o entidad que tiene aprobada responsabilidad de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo. El término *propietario* no se refiere a que la persona realmente tiene alg ún derecho de propiedad sobre el activo.

Tabla A.1 (continuación)

A.7.2 Clasificación de la información		
Objetivo: Garantizar que la información reciba un apropiado nivel de protección.		
A.7.2.1	Directrices para la clasificación	Control La información se debe clasificar en términos de su valor, requerimientos legales, sensibilidad, y criticidad para la organización.
A.7.2.2	Rotulado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para rotular y manipular la información, en concordancia con el esquema de clasificación adoptado por la organización.
A.8 Seguridad de los Recursos Humanos		
A.8.1 Antes de emplear[4]		
Objetivo: Asegurar que los empleados, contratistas y usuarios de tercera parte entiendan sus responsabilidades, sean adecuados para los roles para los cuales son considerados, y para reducir el riesgo de hurto, fraude o el mal uso de las instalaciones.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y usuarios de tercera parte en concordancia con la política de seguridad de la información de la organización.
A.8.1.2	Selección	Control La verificación de antecedentes de los candidatos para el puesto, contratistas, y usuarios de tercera parte, debe ser registrada y llevada a cabo en concordancia con las leyes correspondientes, regulaciones y reglas éticas, y deben ser proporcionales a los requerimientos del negocio, a la clasificación de la información a ser accedida, y los riesgos detectados.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de sus obligaciones contractuales, los empleados, contratistas y los usuarios de tercera parte deben estar de acuerdo y firmar los términos y condiciones de sus contratos de empleo, los cuales deben reflejar sus responsabilidades y las de la organización para con la seguridad de la información.
A.8.2 Durante el empleo		
Objetivo: Asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y preocupaciones de la seguridad de la información, sus responsabilidades y obligaciones, y estén preparados para respaldar las políticas de seguridad organizacional en el curso de su trabajo normal, y para reducir el riesgo de error humano.		
A.8.2.1	Responsabilidades de la dirección	Control La dirección debe requerir a los empleados, contratistas y usuarios de tercera parte que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización.
A.8.2.2	Concienciación, educación y entrenamiento en seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas y usuarios de tercera parte deben recibir una apropiada concientización y actualizaciones regulares en las políticas y procedimientos organizacionales, que sean importantes para su tarea.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que hayan generado un incidente de seguridad.

(Continúa)

[4] Explicación: la palabra *emplear* se utiliza aquí para cubrir todas las situaciones siguientes:
Emplea a gente (temporaria o permanente), nombramientos de personal (cambio de roles de trabajo, asignación de contratos) o la terminación de cualquiera de éstas situaciones.

Tabla A.1 (continuación)

A.8.3 Desvinculación o cambio de puesto		
Objetivo: Asegurar que los empleados, contratistas y usuarios de tercera parte abandonen la organización o cambien de empleo de una manera ordenada .		
A.8.3.1	Responsabilidades de la finalización	Control Las responsabilidades para realizar la desvinculación o cambio de puesto deben estar claramente definidas y asignadas.
A.8.3.2	Retorno de activos	Control Todos los empleados, contratistas y usuarios de tercera parte deben devolver todos los activos de la organización en su poder tras la terminación de su empleo, contrato, o acuerdo.
A.8.3.3	Remoción de derechos de acceso	Control Se deben revisar los derechos de acceso de todos los empleados, contratistas y usuarios de tercera parte a las instalaciones de procesamiento de la información tras la finalización de su empleo, contrato o acuerdo, o deben ser adaptados tras algún cambio.
A.9 Protección física y ambiental		
A.9.1 Áreas seguras		
Objetivo: Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se deben usar perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjetas o escritorios de recepción atendidos por personas), para proteger áreas que contengan información e instalaciones del procesamiento de información.
A.9.1.2	Controles de acceso físico	Control Las áreas seguras deben ser resguardadas por controles de acceso adecuados que garanticen que sólo se permite el acceso a personal autorizado.
A.9.1.3	Aseguramiento de oficinas, recintos e instalaciones	Control Se debe diseñar y aplicar seguridad física para oficinas, recintos e instalaciones.
A.9.1.4	Protección contra amenazas externas y del ambiente	Control Se debe designar y aplicar la protección física contra daños potenciales causados por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o desastre provocado por el hombre.
A.9.1.5	Trabajo en áreas protegidas	Control Se debe diseñar y aplicar protección física y las directrices para el trabajo en áreas protegidas.
A.9.1.6	Áreas de acceso público, de entrega y de carga	Control Se deben controlar los puntos de acceso, como las áreas de entrega y carga y otros puntos donde personas sin autorización pueden llegar a entrar a las instalaciones y, de ser posible, se deben aislar de las instalaciones de procesamiento o de información para evitar el acceso no autorizado.
A.9.2 Seguridad del equipamiento		
Objetivo: Impedir pérdidas, daños, robos o exposiciones al riesgo de los activos así como impedir la interrupción de las actividades de la empresa.		
A.9.2.1	Ubicación y protección del equipamiento	Control El equipamiento debe ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales y oportunidades de accesos no autorizados.

(Continúa)

Tabla A.1 (continuación)

A.9.2.2	Elementos de soporte	Control El equipamiento debe encontrarse protegido con respecto a fallas en el suministro de energ ía u otras fallas en elementos de soporte.
A.9.2.3	Seguridad del cableado	Control El cableado de energía y el de telecomunicaciones que transporta datos o da soporte a ser vicios de información deben ser protegidos de intercepciones o da ños.
A.9.2.4	Mantenimient o del equipo	Control El equipo debe recibir el correcto mantenimiento para asegurar su disponibilidad e integridad continuas.
A.9.2.5	Seguridad del equipamiento fuera del ámbito de la organización	Control Se debe aplicar seguridad al equipamiento que est é fuera del ámbito de la organización teniendo en cu enta los diferentes riesgos de trabajar fuera del terreno de la organización.
A.9.2.6	Baja segura o reutilización de equipamiento	Control Todas las partes de equipamiento que contengan un medio de almacenamiento deben ser verificadas para asegurar que se ha quitado o sobreescrito, previo a la baja, cualquier dato sensible y licencia de soft ware.
A.9.2.7	Retiro de bienes	Control El equipamiento, la información o el software no deben ser sacados del predio sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos operati vos y responsabilidades Objetivo: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.		
A.10.1.1	Documentación de los procedimientos operativos	Control Los procedimientos operativos se deben documentar, mantener y encontrar disponibles para todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambios	Control Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información.
A.10.1.3	Segregación de funciones	Control Las funciones y las áreas de responsabilidad deben encontrarse separadas para reducir las oportunidades de modificaciones sin autorización o no intencionales, o una mala utilización de los activos de la organización.
A.10.1.4	Separación de las instalaciones de desarrollo, de pruebas y operacionales	Control Las instalaciones de desarrollo, de pruebas y operacionales deben encontrarse separadas para reducir los riesgos de accesos no autorizados o cambios en los sistemas operacionales.
A.10.2 Gestión de la entrega de servicio por terceras partes Objetivos: Implementar y mantener el nivel adecuado de seguri dad de información y la provisión de servicio en línea con los acuerdos de entrega de servicio por terceras partes.		
A.10.2.1	Provisión de servicio	Control Se debe asegurar que los controles de seguridad, las definiciones de servicio y niveles de entrega incluidos en el acuerdo de provisión de servicio de la tercera parte sean implementados, operados, y mantenidos por la tercera parte.
A.10.2.2	Seguimiento y revisi ón de los servicios de terceras partes	Control Los servicios, reportes y registros provistos por terceras partes deben ser seguidos, controlados y revisados de manera regular, así como también se deben llevar a cabo auditorías de manera regular.

(Continúa)

Tabla A.1 (continuación)

A.10.2.3	Gestión del cambio de los servicios de terceras partes	Control Los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras a las políticas, procedimientos y controles de seguridad de la información existentes, deben ser gestionados teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la reevaluación del riesgo.
A.10.3 Planificación y aceptación de sistemas Objetivo: Minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	Gestión de la capacidad	Control El uso de recursos debe ser controlado y ajustado, y se deben realizar proyecciones de futuros requerimientos de capacidad para asegurar el desempeño requerido de los sistemas.
A.10.3.2	Aprobación del sistema	Control Se deben establecer criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones, así como también pruebas adecuadas para los sistemas, llevadas a cabo durante el desarrollo, y previas a la aceptación.
A.10.4 Protección contra código malicioso y código móvil Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra código malicioso	Control Se deben implementar los controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de los usuarios.
A.10.4.2	Controles contra código móvil	Control Cuando el código móvil esté autorizado, la configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe prevenir la ejecución de código móvil no autorizado.
A.10.5 Resguardo Objetivo: Mantener la integridad y la disponibilidad de la información y de las instalaciones del procesamiento de la información.		
A.10.5.1	Resguardo de la Información	Control Se deben tomar copias de resguardo de la información y del software y se deben probar regularmente en concordancia con la política acordada de resguardo.
A.10.6 Gestión de la seguridad de la red Objetivo: Garantizar la seguridad de la información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de redes	Control Las redes deben estar adecuadamente administradas y controladas, con la intención de protegerlas de amenazas, y para mantener la seguridad para los sistemas y las aplicaciones que las utilizan, 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 servicios de redes las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de redes, ya sean servicios provistos por la organización o tercerizados.
A.10.7 Manejo de los medios de comunicación Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de los activos, y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de medios removibles	Control Deben existir procedimientos para la gestión de medios informáticos removibles.

(Continúa)

Tabla A.1 (continuación)

A.10.7.2	Eliminación de medi os informáticos	Control Se deben eliminar los medios de forma segura y protegida utilizando procedimientos formales cuando no contin úen siendo requeridos.
A.10.7.3	Procedimientos del manejo de información	Control Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada.
A.10.7.4	Seguridad de la documentación del sistema	Control La documentación del sistema debe ser protegida contra accesos no autorizados.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y el software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Políticas y procedimientos de intercambio de la información	Control Se deben establecer políticas , procedimientos y controles formales para proteger el intercambio de información a trav és del uso de todos los tipos de las inst alaciones de comunicación.
A.10.8.2	Acuerdo de intercambio	Control Se deben establecer acuerdos de intercambio de la información y del software entre la organización y las terceras partes.
A.10.8.3	Medio físico en tránsito	Control Se deben proteger los medios que contengan información contra accesos no autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de la organización.
A.10.8.4	Mensajería electrónica	Control Se debe proteger de forma adecuada la información involucrada en los mensajes electrónicos.
A.10.8.5	Sistemas de informa ción del 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: Garantizar la seguridad de los servicio s de comercio electrónicos, y su uso seguro.		
A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que pasa por las redes públicas se debe encontrar protegida de actividades fraudulentas, disputas de contrato, y divulgaciones y modificaciones no autorizadas.
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea se debe encontrar protegida para prevenir transacciones incompletas, que sean erróneamente direccionadas, alteraciones no autorizadas de mensajes, divulgaciones no autorizadas, duplicación o repetición no autorizada de mensajes.
A.10.9.3	Información públicamente disponible	Control Se debe proteger la integridad de la información que está disponible públicamente para prevenir modificaciones no autorizadas.
A.10.10 Seguimiento y control Objetivo: Detectar las actividades no autorizadas de procesamiento de información.		

(Continúa)

Tabla A.1 (continuación)

A.10.10.1	Registro de auditoría	Control Se deben producir y mantener regi stros de auditorías en los cuales se registren las acti vidades, excepciones, y eventos de seguridad de los usuarios, por un período acordado para ayudar en futuras investigaciones y el seguimiento del control de acceso.
A.10.10.2	Seguimiento del us o del sistema	Control Se deben establecer procedimientos para el uso de las instalaciones de procesamiento de informaci ón y se deben revisar de forma regular los resultados de las actividades de seguimiento.
A.10.10.3	Protección de la información de los registros de actividad	Control Las instalaciones de registro y la información de registro deben estar protegidas contra la manipulación y procesos no autori zados.
A.10.10.4	Registros de la actividad de administrador y operador	Control Se debe llevar registro de las actividades del administrador del sistema y del operador del sistema.
A.10.10.5	Registro de acciones fallidas	Control Se debe llevar un registro de las fallas, las mismas deben ser analizadas y se deben tomar las acciones apropiadas.
A.10.10.6	Sincronización del reloj	Control Dentro de una organización o dominio de seguridad los relojes de todos los sistemas de procesamiento de información se deben encontrar sincronizados de acuerdo a una fuente de tiempo precisa, previamente convenida.
A.11 Control de accesos		
A.11.1 Requerimientos para el control de accesos Objetivo: Controlar el a cceso 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 basada en los re querimientos de acceso, de seguridad y del negocio.
A.11.2 Administración de accesos de usuarios Objetivo: Asegurar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas de Información.		
A.11.2.1	Registro de usuarios	Control Debe existir un procedimiento formal de registro de alta y baja de registros para otorgar y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Administración de privilegios	Control La asignación y el uso de los privilegios debe ser restringido y controlado.
A.11.2.3	Administración de las contrase ñas de usuario	Control La asignación de contraseñas debe ser controlada mediante un proceso formal de gestión.
A.11.2.4	Revisión de los derec hos de acceso	Control La alta dirección debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Prevenir el acceso de usuarios no autorizados de mo do que la información y las instalaciones de procesamiento de la información, no sean comprometidas o sustraidas.		
A.11.3.1	Uso de contraseñas	Control Se debe solicitar a los usuarios que sigan las buenas pr ácticas de seguridad en la selección y uso de contraseñas.

(Continúa)

Tabla A.1 (continuación)

A.11.3.2	Equipamiento de usuario que se deja desatendido	Control Los usuarios se deben asegurar que el equipamiento desatendido tenga protección adecuada.
A.11.3.3	Política de pantalla y escritorio limpios	Control Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento remo vibles y una política de pantalla limpia para las instalaciones de procesamiento de la in formación.
A.11.4 Control de acceso a la red Objetivo: Prevenir el acceso no autorizado a los servicios de red.		
A.11.4.1	Política de utilización de los servicios de red	Control Se debe proveer a los usuarios solo el acceso a los servicios para los cuales han sido específicamente autorizados.
A.11.4.2	Autenticación de usuarios para conexiones externas	Control Se deben utilizar m étodos de aut enticación apropiados para el control de acceso de usuarios remotos.
A.11.4.3	Identificación del equipamiento en redes	Control Se debe considerar la identificación autom ática de equipamiento como un medio para autenticar conexiones de ubicaciones y equipamiento específicos.
A.11.4.4	Protección de los puertos de diagnóstico y configuración remotos	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.
A.11.4.5	Separación en redes	Control Los grupos de servicios de la información , usuarios y sistemas de información se deben subdividir en redes.
A.11.4.6	Control de conexión a la red	Control Para redes compartidas, especialmente aquellas que se extienden a través de los límites de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, alineadas con la política de control de acceso y con los requerimientos de las aplicaciones comerciales (ver 11.1).
A.11.4.7	Control de enrutamiento de red	Control Los controles de enrutamiento se deben implementar en redes para garantizar que las conexiones informáticas y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema operativo Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos seguros de inicio de sesión ("log-on")	Control El acceso a los sistemas operativ os debe ser controlado por un procedimiento seguro de inicio de sesión.
A.11.5.2	Identificación y autenticación de usuarios	Control Todos los usuarios deben tener un único identificador (identificador de usuario) para su uso personal, y se debe elegir una técnica adecuada de autenticación para sustanciar la identidad declarada por el usuario.
A.11.5.3	Sistema de administración de contraseñas	Control Los sistemas que administran contraseñas deben ser interactivos y deben garantizar contraseñas de calidad.

(Continúa)

Tabla A.1 (continuación)

A.11.5.4	Uso de utilitar ios de siste ma	Control El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles de las aplicaciones o del sistema de be ser restringido y controlado de cerca.
A.11.5.5	Expiración de la sesión	Control Las sesiones inactivas se deben cerrar luego de un período definido de inactividad.
A.11.5.6	Limitaciones del tiempo de conexión	Control Se deben utilizar restricciones acerca del tiempo de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones y a la información		
Objetivo: Prevenir el acceso no autorizado a la info rmación contenida en los sistemas de aplicación.		
A.11.6.1	Restricción de acce so a la información	Control Se debe restringir el acceso a la información y a las funciones de los sistemas de aplicación a los usuarios y al personal de soporte de acuerdo con una política de control de acceso definida.
A.11.6.2	Aislamiento de sist emas sensibles	Control Los sistemas sensibles se deben encontrar en un ambiente inform ático dedicado (aislado).
A.11.7 Computación móvil y teletrabajo		
Objetivo: Garantizar la seguridad de la información mientras se utiliza computación móvil e instalaciones de teletrabajo.		
A.11.7.1	Computación y comunicaciones móviles	Control Se debe establecer una política formal y se deben adoptar medidas de seguridad adecuadas para protegerse contra los riesgos del uso de dispositivos de computación e instalaciones de comunicación móviles.
A.11.7.2	Teletrabajo	Control Se debe desarrollar e implementar una política , planes y procedimientos operacionales para las actividades de teletrabajo.
A.12 Adquisición, desarrollo y mant enimiento de Sistemas de Información		
A.12.1 Requerimientos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificaciones de los requerimientos de seguridad	Control Las declaraciones de requerimientos comerciales para nuevos sistemas de información, o mejoras de los sistemas de información existentes, deben especificar la s necesidades de controles de seguridad.
A.12.2 Correcto procesamiento en las aplicaciones		
Objetivo: Prevenir errores, p érdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de entrada de datos	Control La entrada de datos a las aplicaciones deben ser validados para asegurar que estos datos son correctos y apropiados.
A.12.2.2	Controles de proces amiento interno	Control Se deben incorporar las verificaciones de validación a las aplicaciones para detectar cualquier caso de corrupción de la información a través del procesamiento de errores o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimi entos para asegurar la autenticidad y para proteger la integridad del mensaje de las aplicaciones, y se deben identificar e implementar controles apropiados.

(Continúa)

Tabla A.1 (continuación)

A.12.2.4	Validación de los datos de salida	Control Se debe validar la salida de datos de una aplicación para garantizar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad, y la integridad de la información por medios criptogr áficos.		
A.12.3.1	Política de utilización de controles criptográficos	Control Se debe desarrollar e implementar una política para el uso de con - troles criptográficos para la protección de la información.
A.12.3.2	Administración de claves	Control Se debe establecer la gestión de claves para dar soporte al uso organizacional de técnicas criptográficas.
A.12.4 Seguridad de los archivos de sistema Objetivo: Garantizar la seguridad de los archivos de sistema.		
A.12.4.1	Control del soft ware operacional	Control Deben existir procedimientos para controlar la instalación de software en sistemas operacionales.
A.12.4.2	Protección de los datos de prueba del sistema	Control Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
A.12.4.3	Control de acceso al código fuente de programa	Control Se debe restringir el acceso al código fuente de programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.		
A.12.5.1	Procedimientos de control de cambios	Control La implementación de cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad organizacional.
A.12.5.3	Restricción del cambio en los paquetes de software	Control Las modificaciones a los paquetes de software deben ser desalentadas, limitadas a los cambios necesarios, y todos los cambios deben ser estrictamente controlados.
A.12.5.4	Fuga de la información	Control Se deben prevenir las oportunidades de fuga de la información.
A.12.5.5	Desarrollo tercerizado de software	Control El desarrollo externo de software debe ser supervisado, seguido y controlado por parte de la organización.
A.12.6 Gestión de las vulnerabilidades técnicas Objetivo: Reducir el riesgo resultante de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de las vulnerabilidades técnicas	Control Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que son utilizados, se debe evaluar la exposición de la organización a tales vulnerabilidades, y se deben tomar las medidas adecuadas para tratar los riesgos asociados.

(Continúa)

Tabla A.1 (continuación)

A.13 Gestión de los incidentes de la seguridad de la información		
A.13.1 Informe de los eventos y debilid ades de la seguridad de la información Objetivo: Garantizar que los eventos de seguridad de la in formación y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se a pliquen las acciones correctivas en el tiempo correcto .		
A.13.1.1	Reporte de los eventos de la seguridad de la información	Control Los eventos de seguridad de la información deben ser reportados mediante canales de gestión apropiados tan pronto como sea posible.
A.13.1.2	Reporte de las debilidades de la seguridad	Control Se debe requerir que todos los empleados, contratistas y usuarios de tercera parte de los sistemas y servicios de información tomen nota y reporten cualquier acción sospec hosa que observen o consideren que está relacionada con las debilidades de seguridad de los sistemas o de los servicios.
A.13.2 Gestión de los incidentes y mejo ras de la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efec tivo a la gestión de incidentes de seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer los procedimientos y gestión de las responsabilidades para garantizar una respue sta rápida, efectiva y ordenada de los incidentes de seguridad de la información.
A.13.2.2	Aprendiendo a partir de los incidentes de la seguridad de la información	Control Deben existir mecanismos para permitir que se cuantifiquen y supervisen los tipos, vol úmenes, y costos de los incidentes de la seguridad de la información.
A.13.2.3	Recolección de la evidencia	Control Cuando se lleve a cabo un seguimiento sobre una persona u organización después de que haya ocurrido un incidente de seguridad de la información que involucre acciones legales (ya sea civil o criminal), se debe recolectar, retener y presentar evidencia para cumplir con los requerimientos legales en la jurisdicción que corresponda.
A.14 Gestión de la continuidad del negocio		
A.14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio Objetivo: Contrarrestar las interrupciones de las actividades de la organización y proteger los procesos cr íticos del negocio de los efectos de las fallas significativas de los sistemas de información o desastres y para asegurar su reanudación oportuna.		
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control Se debe desarrollar y mantener un proceso de gestión que dirija los requerimientos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación de los riesgos	Control Se deben identificar los eventos que pueden causar interrupciones a los procesos del negocio, junto con la probabilidad y el impacto de tales interrupciones y sus consecuencias a la seguridad de la información.
A.14.1.3	Elaboración e implementación de planes que incluyan la seguridad de la información	Control Los planes deben ser desarrollados e implementados para mantener o restablecer las operaciones y asegurar la disponibilidad de la información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de los procesos críticos del negocio.

(Continúa)

Tabla A.1 (continuación)

A.14.1.4	Marco para la planificación de la continuidad del negocio	Control Se debe mantener un marco único de planes para la continuidad del negocio, para garantizar que todos los planes son consistentes, para cumplir con los requerimientos de seguridad de la información en forma consistente, y para identificar las prioridades de las pruebas y el mantenimiento.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad de los negocios	Control Los planes de continuidad de los negocios deben ser probados y actualizados periódicamente para garantizar que se encuentran al día y continúan siendo efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento de requerimientos legales Objetivo: Impedir infracciones y violaciones de cualquier obligación legal, reglamentaria, reguladora o contractual, y de cualquier requerimiento de seguridad.		
A.15.1.1	Identificación de la legislación aplicable	Control Todos los requerimientos legales, normativos y contractuales pertinentes, así como el enfoque de la organización para cumplir con estos requerimientos, deben estar definidos y documentados y se deben mantener actualizados para cada sistema de información, y para la organización
A.15.1.2	Derechos de propiedad intelectual (IPR) NOTA IRAM. Por sus siglas en inglés (Intellectual property rights)	Control Se deben implementar los procedimientos apropiados para garantizar el cumplimiento con los requerimientos legislativos, regulatorios y contractuales referidos al uso del material sobre el cual puede existir un derecho de propiedad intelectual y sobre el uso de productos de software propietario.
A.15.1.3	Protección de los registros de la organización	Control Los registros importantes deben ser protegidos contra pérdida, destrucción y falsificación, en concordancia con los requerimientos legales, regulatorios, contractuales y comerciales.
A.15.1.4	Protección de los datos y privacidad de la información personal	Control La protección y privacidad de los datos debe estar garantizada según se requiera en las legislaciones y regulaciones relevantes, y si es el caso, en las cláusulas contractuales.
A.15.1.5	Prevención contra el mal uso de las instalaciones de procesamiento de la información	Control Se debe disuadir a los usuarios de utilizar las instalaciones de procesamiento de la información para propósitos no autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Los controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, leyes, y regulaciones vigentes.
A.15.2 Cumplimiento con las políticas y normas de seguridad, y el cumplimiento técnico Objetivo: Garantizar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización.		
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	Control Los responsables deben garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para alcanzar el cumplimiento con las políticas y normas de seguridad.
A.15.2.2	Verificación del cumplimiento técnico	Control Los sistemas de información deben ser verificados periódicamente para garantizar que cumplen con las normas de implementación de la seguridad.

(Continúa)

Tabla A.1 (fin)

A.15.3 Consideraciones de auditorías de sistemas de información Objetivo: Maximizar la efectividad y minimizar la terferen cia hacia y desde el proceso de auditoría de sistemas de información.		
A.15.3.1	Controles de auditoría de sistemas de información	Control Los requerimientos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el ries go de interrupción de los procesos de 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 a fin de evitar cualquier mal uso o el compromiso de ellas.

Anexo B
(Informativo)

Principios de la OCDE y de esta norma

Los principios presentados en las Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información [1] 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 apartados 4, 5, 6 y 8, como se indica en la tabla B.1.

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

Principio OCDE	Proceso de SGSI correspondiente y fase de PHVA
Toma de conciencia Se recomienda que los participantes estén conscientes de la necesidad de seguridad de los sistemas y redes de información y de lo que pueden hacer para mejorar la seguridad.	Esta actividad es parte de la fase *Hacer* (véanse los apartados 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables por la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase *Hacer* (véanse los apartados 4.2.2 y 5. 1)
Respuesta Se recomienda que los participantes act úen de una manera oportuna y en cooperación para evitar , detectar y responder ante incidentes de seguridad.	Ésta es en parte una actividad de seguimiento de la fase *Verificar* (véanse los apartados 4. 2.3 y 6 a 7.3) y una actividad de respuesta de la fase *Actuar* (véanse los apartados 4.2.4 y 8.1 a 8.3). Esto también se puede cubrir por algunos aspectos de las fases *Planificar* y *Verificar*.
Valoración de riesgos Se recomienda que los participantes realicen valoraciones de los riesgos.	Esta actividad es parte de la fase *Planificar* (véase el apartado 4.2.1) y la revaloración del riesgo es parte de la fase *Verificar* (véanse los apartados 4.2.3 y 6 a 7.3).
Diseño e implementación de la seguridad Se recomienda que los participantes incorporen la seguridad como un elemento esencial de los sistemas y redes de información.	Una vez que se ha realizado la valoración de riesgos, se seleccionan controles para el tratamiento de riesgos como parte de la fase *Planificar* (véase el apartado 4.2.1). La fase *Hacer* (véanse los apartados 4.2.2 y 5.2) cubre la implementación y el uso operacional de estos controles.
Gestión de la seguridad Es conveniente que los participantes adopten un enfoque amplio hacia la gestión de la seguridad.	La gestión de riesgos es un proceso que incluye la prevención, detección y respuesta a incidentes, mantenimiento, auditorías y revisión continuos. Todos estos aspectos están cobijados en las fases de *Planificar, Hacer, Verificar y Actuar*.
Revaloración Es conveniente que los participantes revisen y revaloren la seguridad de los sistemas y redes de información, y realicen las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos de seguridad.	La revaloración de la seguridad de la información es una parte de la fase *Verificar* (véanse los apartados 4.2.3 y 6 a 7.3), en donde se deberían realizar revisiones regulares para verificar la eficacia del sistema de gestión de la seguridad de la información ; y la mejora de la seguridad es parte de la fase *Actuar* (véanse los apartados 4.2.4 y 8.1 a 8.3).

Anexo C
(Informativo)

Correspondencia entre la IRAM-ISO 9001:2000, la IRAM-ISO 14001:2005, y la presente norma

La tabla C.1 muestra la correspondencia entre la IRAM-ISO 9001:2000, la IRAM-ISO 14001:2005 y la presente norma.

Tabla C.1 - Correspondencia entre la IRAM-ISO 9001:2000, la IRAM-ISO 14001:2005 y la presente norma

Esta norma	IRAM-ISO 9001:2000	IRAM-ISO 14001:2005
0 Introducción	**0. Introducción**	Introducción
0.1 Generalidades	0. 1 Generalidades	
0.2 Enfoque basado en procesos	0.2 Enfoque basado en procesos	
	0.3 Relación con la norma ISO 9004	
0.3 Compatibilidad con otros sistemas	0.4 Compatibilidad con otros sistemas de gestión	
1 Objeto	**1. Alcance**	**1. Objeto y campo de aplicación**
1.1 Generalidades	1. 1 Generalidades	
1.2 Aplicación	1.2 Aplicación	
2 Documentos normativos para consulta	**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. Sistema de gestión de la calidad**	**4. Requisitos del sistema de gestión ambiental**
4.1 Requisitos generales	4.1 Requisitos generales	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		
4.2.2 Implementación y operación del SGSI		4.4 Implementación y operación
4.2.3 Seguimiento y revisión del SGSI	8.2.3 Seguimiento y medición de los procesos	4.5.1 Seguimiento y medición
	8.2.4 Seguimiento y medición del producto	

(Continúa)

Tabla C.1 (continuación)

Esta norma	**IRAM-ISO 9001:2000**	**IRAM-ISO 14001:2005**
4.2.4 Mantenimiento y mejora del SGSI		
4.3 Requisitos de documentación	**4.2 Requisitos de documentación**	
4.3.1 Generalidades	4.2.1 Generalidades	
	4.2.2 Manual de calidad	
4.3.2 Control de documentos	4.2.3 Control de documentos	4.4.5 Control de documentos
4.3.3 Control de registros	4.2.4 Control de registros	4.5.4 Control de registros
5 Responsabilidad de la dirección	**5. Responsabilidad de la dirección**	
5.1 Compromiso de la dirección	5.1 Compromiso de la dirección	
	5.2 Enfoque al cliente	
	5.3 Política de calidad	4.2 Política ambiental
	5.4 Planificación	4.3 Planificación
	5.5 Responsabilidad, autoridad y comunicación	
5.2 Gestión de recursos	**6. Gestión de los recursos**	
5.2.1 Provisión de recursos	6.1 Provisión de recursos	
	6.2 Recursos humanos	
5.2.2 Formación, toma de conciencia y competencia	6.2.2 Competencia, toma de conciencia y formación	4.2.2 Competencia, formación y toma de conciencia
	6.3 Infraestructura	
	6.4 Ambiente de trabajo	
6 Auditorías internas del SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7 Revisión del SGSI por la dirección	5.6 Revisión por la dirección	4.6 Revisión por la dirección
7.1 Generalidades	5.6.1 Generalidades	
7.2 Información para la revisión	5.6.2 Información para la revisión	
7.3 Resultados de la revisión	5.6.3 Resultados de la revisión	
8. Mejora del SGSI	**8.5 Mejora**	
8.1 Mejora continua	8.5.1 Mejora continua	
8.2 Acción correctiva	8.5.3 Acciones correctivas	4.5.3 No conformidad, acción correctiva y acción preventiva

(Continúa)

Tabla C.1 (fin)

Esta norma	**IRAM-ISO 9001:2000**	**IRAM-ISO 14001:2005**
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles		**Anexo A Orientación para el uso de esta norma**
Anexo B Principios de la OCDE y esta norma		
Anexo C Correspondencia entre la IRAM-ISO 9001:2000, la IRAM-ISO 14001:2005 y esta norma	**Anexo A Correspondencia entre la IRAM-ISO 9001:2000 y la IRAM-ISO 14001:2005**	**Anexo B Correspondencia entre la IRAM-ISO 14001:2005 y la IRAM-ISO 9001:2000**

Anexo D
(Informativo)

Bibliografía de la ISO/IEC 27001

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

[2] ISO/IEC 13335-1:2004, Information Technology. Part 1: Concepts and Models for Information and Communications Technol ogy Security Management.

[3] ISO/IEC TR 13335-3:199 8, 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 Requirem ents for Bodies Operating Assessment and Certification/registration of Quality Systems.

[9] ISO/IEC Guide 73:2002, Ris k Management. Vocabulary. Guidelines for use in Standards.

Otras publicaciones

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

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

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

Anexo E - IRAM
(Informativo)

Bibliografía

En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
ISO/IEC 27001:2005 - Information technology. Security techniques. Information security management systems. Requirements.

Anexo F - IRAM
(Informativo)

Integrantes de los organismos de estudio

El estudio de esta norma ha estado a cargo de los organismos respectivos, integrados en la forma siguiente:

Subcomité de Seguridad en tecnología de la información

Integrante		Representa a:
Lic.	Alberto David AIRALA	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN
Sr.	Gustavo ALDEGANI	INVITADO ESPECIAL
Lic.	Julio C. BELLENE	GRUPO TEKNE
Sr.	Raúl Eduardo CABRERA	INVITADO ESPECIAL
Ing.	Jorge M. CANALE	CITEFA – INSTITUTO DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS DE LAS FUERZAS ARMADAS
Sra.	Carolina CASTRO	X-PROJECT S.A.
Ing.	Jorge Luis CEBALLOS	CONSULTORA EMPRENDER
Sr.	Ricardo CIUFFA	AySA – AGUA Y SANEAMIENTO ARGENTINO
Sr.	Omar CLAVER	MINISTERIO DE ECONOMÍA DE LA PCIA. DE BUENOS AIRES
Lic.	Adriana DE ROSE	INVITADO ESPECIAL
Sr.	Guillermo Eduardo DÍAZ	SECCURACY
Ing.	Norberto ESARTE	GATECH S. R. L.
Ing.	Jorge ETEROVIC	CAJA DE VALORES S. A.
Sra.	Lorena FERREYRO	OSDE BINARIO
Sr.	Marco Damian FIORENTINO	NACIÓN AFJP
Sra.	Graciela FRIGERI	INVITADO ESPECIAL
Lic.	Sebastián GAGLIARDI	BDO BECHER S.R.L.
Sr.	Gabriel GORDON	MICROSOFT DE ARGENTINA S.A.
Ing.	Gustavo GUIÑAZU	BANCO DE LA PROVINCIA DE BS. AS.
Cont.	Silvia IGLESIAS	IGLESIAS, RUBIO & ASOC.
Ing.	Roberto LANGDON	CPCI – CONSEJO PROFESIONAL DE CIENCIAS INFORMÁTICAS
Ing.	Liliana Rosa MIRA	LMIRA CONSULTORES
Lic.	Gisella MORODER	KHU TECHNOLOGIES S.A.
Sr.	Marcos PASSARELLO	INVITADO ESPECIAL
Sr.	Fernando RADICCHI	BNA – BANCO DE LA NACIÓN ARGENTINA
Sr.	Leonardo RAMOS	MINISTERIO DE ECONOMÍA DE LA PCIA. DE BUENOS AIRES
Ing.	Pablo Miguel ROMANOS	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN
Sra.	Sandra RUBIO	IGLESIAS, RUBIO & ASOC.
Sr.	José Emmanuel SFEIR	INSTITUTO UNIVERSITARIO DE LA POLICÍA FEDERAL ARGENTINA
Mg.	Paula ANGELERI	IRAM
Lic.	Marta R. de BARBIERI	IRAM

Integrante		Representa a:
Lic.	Pedro Claudio COSTA	IRAM
Lic.	Domingo DONADELLO	IRAM
Ing.	Sergio Fabian ROJAS	IRAM

Comité General de Normas (C.G.N.)

Integrante		Integrante	
Dr.	Víctor ALDERUCCIO	Ing.	Jorge MANGOSIO
Dr.	José M. CARACUEL	Tco.	Hugo D. MARCH
Lic.	Alberto CERINI	Ing.	Samuel MARD YKS
Ing.	Ramiro FERNÁNDEZ	Ing.	Tulio PALACIOS
Dr.	Federico GUITAR	Tco.	Ángel TESTORELLI
Ing.	Jorge KOSTIC	Ing.	Raúl DELLA PORTA

ICS 35.040
* CNA 00.00

* Corresponde a la Clasificación Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación del Ministerio de Defensa.