TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - REQUISITOS

1. OBJETIVOS

Esta Norma especifica los requisitos para establecer, implantar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el contexto de la organización. Esta Norma también incluye los requisitos para la evaluación y tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. No es aceptable la exclusión de cualquiera de los requisitos especificados en los Capítulos 4 al 10 cuando una organización declara conformidad con la presente Norma.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos, en su totalidad o en parte, están referenciados normativamente en este documento y son indispensables para su aplicación. Para las referencias fechadas, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento referenciado (incluyendo cualquier modificación).

ISO/IEC 27000, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.*

3. TÉRMINOS Y DEFINICIONES

Para el propósito de este documento, son aplicables los términos y definiciones dados en la Norma ISO/IEC 27000.

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprender la organización y su contexto

La organización debe determinar los asuntos externos e internos que son relevantes para su propósito y que afectan su capacidad de lograr el (los) resultados (s) deseado (s) de su sistema de gestión de la seguridad de la información.

Nota: La determinación de estos asuntos se refiere a establecer el contexto interno y externo de la organización, considerado en el apartado 5.3 de la Norma ISO 31000, Gestión de riesgos - Principios y directrices.

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) Las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información;
b) Los requisitos de estas partes interesadas respecto de la seguridad de la información.

Nota: Los requisitos de las partes interesadas pueden incluir requisitos legales y reglamentarios y obligaciones contractuales.

4.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

a) los problemas externos e internos mencionados en 4.1;
b) los requisitos mencionados en 4.2; y
c) las interfaces y dependencias entre actividades desempeñadas por la organización y aquellas que son desempeñadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de la seguridad de la información

La organización debe establecer, implantar, mantener y mejorar continuamente su sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.

5. LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe determinar su liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que la política de seguridad de la información y los objetivos de seguridad de la información se encuentran establecidos y son compatibles con la dirección estratégica de la organización.;
b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;
c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información se encuentren disponibles;
d) comunicando la importancia de la gestión efectiva de la seguridad de la información y de cumplir con los requisitos del sistema de gestión de la seguridad de la información;
e) asegurando que el sistema de gestión de la seguridad de la información alcance sus resultados previstos;
f) dirigiendo y apoyando a que las personas contribuyan con la efectividad del sistema de gestión de la seguridad de la información;
g) promoviendo la mejora continua; y
h) apoyando otros roles de gestión relevante para deformar su liderazgo, como compete a sus áreas de responsabilidad.

5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

a) sea adecuada al propósito de la organización;
b) incluya los objetivos de seguridad de la información (ver 6.2) o proporcione el marco para establecer los objetivos de seguridad de la información;
c) incluya un compromiso para cumplir con los requisitos aplicables relacionados con la seguridad de la información; e
d) incluya un compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información debe:

e) estar disponible como información documentada;
f) ser comprendida dentro de la organización; y
g) estar a disposición de las partes interesadas, según corresponda.

5.3 Roles, responsabilidades y autoridades organizacionales

La alta dirección debe asegurar que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información estén asignadas y comunicadas.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) garantizar que el sistema de gestión de la seguridad de la información cumple con los requisitos de esta Norma; e
b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

Nota: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.

6. APLANIFICACIÓN

6.1 Acciones para hacer frente a los riesgos y oportunidades

6.1.1 Generalidades

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar los aspectos mencionados en 4.1 y los requisitos referidos en 4.2 y determinar los riesgos y oportunidades que necesitan ser gestionados para:

a) asegurar que el sistema de gestión de la seguridad de la información puede alcanzar los resultados previstos;
b) prevenir, o reducir los efectos no deseados; y
c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para gestionar estos riesgos y oportunidades; y
e) cómo:
    1) integrar e implantar las acciones a sus procesos del sistema de gestión de la seguridad de la información; y
    2) evaluar la efectividad de estas acciones.

6.1.2 Evaluación de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

a) establecer y mantener los criterios de riesgos de seguridad de la información que incluyen:
    1) los criterios de aceptación de riesgos; y
    2) los criterios para la realización de las evaluaciones de los riesgos de seguridad de la información;
b) garantice que las reiteradas evaluaciones de los riesgos produzcan resultados consistentes, válidos y comparables;
c) identifique los riesgos de seguridad de la información;
    1) aplique el proceso de evaluación de riesgo de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de la seguridad de la información; e
    2) identifique a los propietarios del riesgo;
d) analice los riesgos de seguridad de la información:
    1) evalúe las consecuencias potenciales que se producirían si los riesgos identificados en 6.1.2 c) 1) llegaran a materializarse;

2) evalúe la probabilidad realista de ocurrencia de los riesgos identificados en 6.1.2 c) 1); y
3) determine los niveles de riesgo;

e) valore los riesgos de seguridad de la información:
1) compare los resultados de los análisis de riesgo con los criterios de riesgos establecidos en 6.1.2 a); y
2) priorice los riesgos analizados para el tratamiento de riesgos.

La organización debe conservar información documentada sobre el proceso de evaluación de riesgos de seguridad de información.

6.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar las operaciones adecuadas de tratamiento de riesgo de seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos;
b) determinar todos los controles que sean necesarios para poner en práctica las operaciones elegidas de tratamiento de riesgos de seguridad de la información;

Nota: Las organizaciones pueden diseñar los controles según sea necesario, o identificarlos de cualquier fuente.

c) comprar los controles determinados en 6.1.3 b) anteriores, con los del Anexo A y verificar que no se han omitido controles necesarios;

Nota 1: El Anexo A contiene una lista completa de objetivos de control y controles elegidos. Los usuarios de esta Norma son referidos al Anexo Apara garantizar que no se pasen por alto los controles necesarios.

Nota 2: Los objetivos de control son incluidos implícitamente en los controles elegidos. Los objetivos de control y los controles incluidos en el Anexo A no son exhaustivos y pueden ser necesarios objetivos de control y controles adicionales.

d) Elaborar una Declaración de Aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) y c)) y la justificación de las inclusiones, sean implantados o no, y la justificación de las exclusiones de los controles del Anexo A;
e) Formular un plan de tratamiento de riesgos de seguridad de la información; y
f) Obtener la aprobación del propietario del riesgo del plan de tratamiento de riesgos de seguridad de la información y aceptación de los riesgos residuales de seguridad de la información.

La organización debe conservar la información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

Nota: El proceso de tratamiento y evaluación de riesgos de seguridad de la información en esta Norma se alinea con los principios y las directrices genéricas proporcionadas con la Norma ISO 31000, Gestión de riesgos - Principios y directrices.

6.2 Objetivos de seguridad de la información y planificación para alcanzarlos

La organización debe establecer objetivos de seguridad de la información en funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) Ser coherentes con la política de seguridad de la información;
b) Ser medibles (mensurables) (si corresponde);

c) Tener en cuenta los requisitos aplicables de seguridad de la información y los resultados de la evaluación de riesgos y del tratamiento de riesgos;
d) Ser comunicados; y
e) Ser actualizados cuando corresponda.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Al planificar como alcanzar estos objetivos de seguridad de la información, la organización debe determinar:

f) Lo que se va a hacer;
g) Qué recursos van a ser necesarios;
h) Quién va a ser responsable;
i) Cuándo se va a completar; y
j) Cómo van a ser evaluados los resultados.

7. SOPORTE

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implantación, el mantenimiento y la mejora continua del sistema de gestión de la seguridad de la información.

7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de la(s) persona(s) que realiza el trabajo bajo su control, que afecta el desempeño de la seguridad de la información;
b) Asegurarse que estas personas son competentes en cuanto a educación, formación o experiencia apropiada;
c) Cuando corresponda, adaptar acciones para adquirir las competencias necesarias, y evaluar la eficacia de las acciones adaptadas; y
d) Conservar la información documentada adecuada como evidencia de la competencia.

Nota: Las acciones aplicables puede incluir, por ejemplo, la provisión de capacitación, la tutoría de, o la reasignación de empleados actuales; o la contratación de personas competentes.

7.3 Toma de conciencia

Las personas que realizan trabajos bajo el control de la organización, deben tener en cuenta:

a) La política de seguridad de la información;
b) Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y
c) Las consecuencias de que no cumplan con los requisitos del sistema de gestión de la seguridad de la información.

7.4 Comunicación

La organización debe determinar la necesidad de las comunicaciones internas y externa pertinentes para el sistema de gestión de la seguridad de la información, incluyendo:

a) qué comunicar;
b) cuándo comunicar;
c) con quién comunicarse;

d) quién debe comunicar;
e) los procesos mediante los cuales se va a establecer la comunicación.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) información documentada requerida por la presente Norma; e
b) información documentada determinada por la organización como necesaria para le eficacia del sistema de gestión de la seguridad de la información.

Nota: El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede variar de una organización a otra debiendo ha:

1) el tamaño de la organización y sus tipos de actividades, procesos y servicios;
2) a complejidad de los procesos y sus interacciones; y
3) la competencia de las personas.

7.5.2 Creación y actualización

Al crear y actualizar información documentada la organización debe garantizar:

a) la identificación y la descripción (por ejemplo, título, fecha, autor o número de referencia);
b) el formato (por ejemplo, el idioma, la versión de software, los gráficos) y los medios (papel, electrónico); y
c) la revisión y aprobación para la conveniencia y suficiencia.

7.5.3 Control de información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por la presenta Norma debe ser controlada para asegurar:

a) que se encuentra disponible para su uso, donde y cuando sea necesario; y
b) que se encuentra protegida adecuadamente (por ejemplo, de la pérdida de confidencialidad, del uso indebido o de la pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

c) la distribución, el acceso, la recuperación y le uso;
d) el almacenamiento y la conservación, incluyendo la preservación de la legibilidad;
e) el control de los cambios (por ejemplo, control de las versiones); y
f) la retención y la disposición.

La información documentada de origen externo, determinada por la organización como necesaria para la planificación y la operación del sistema de gestión de la seguridad de la información, debe ser identificada y controlada, según corresponda.

Nota: El acceso implica una decisión sobre el permiso para ver sólo la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

8. OPERACIÓN

8.1 Planificación y control operacional

La organización debe planificar, implantar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información, y para implantar las acciones determinadas en 6.1. La organización debe poner en práctica planes para alcanzar os objetivos de seguridad de la información determinada en 6.2.

La organización debe mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado según lo previsto.

La organización debe controlar los cambios previstos y revisar las consecuencias de los cambios no deseados, adoptando medidas para mitigar los posibles efectos adversos, según sea necesario.

La organización debe garantizar que los procesos subcontratados son determinados y controlados.

8.2 Evaluación de riesgos de seguridad de la información

La organización debe llevar a cabo evaluaciones de riesgo de seguridad de la información a intervalos planificados o cuando ocurren o se proponen cambios significativos, teniendo en cuenta los criterios establecidos en 6.1.2 a).

La organización debe conservar la información documentada de las evaluaciones de riesgo de seguridad de la información.

8.3 Tratamiento de riesgos de seguridad de la información

La organización debe implantar el plan de tratamiento de riesgos de seguridad de la información.

La organización debe conservar la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) a que se debe hacer seguimiento y medición, incluyendo los procesos y controles de seguridad de la información;
b) los métodos para el seguimiento, la medición, el análisis y al evaluación, según corresponda, para garantizar los resultados válidos;

Nota: Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

c) cuándo se van a llevar a cabo el seguimiento y medición;
d) quién debe realizar el seguimiento y medir;
e) cuándo van a ser evaluados y analizados los resultados del seguimiento y la medición; y
f) quién debe analizar y evaluar esos resultados.

La organización debe conservar la información documentada apropiada como evidencia de los resultados del seguimiento y la medición.

9.2 Auditoría interna

La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) cumple con:
    1) los requisitos propios de la organización para su sistema de gestión de la seguridad de la información; y
    2) los requisitos de la presente Norma;
b) es implementado y mantenido eficazmente.

La organización debe:

c) planificar, establecer, implantar y mantener un programa de auditoría, incluyendo la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la presentación de informes;
d) definir los criterios y el alcance de cada auditoría para cada auditoría;
e) seleccionar los auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proceso de auditoría;
f) garantizar que los resultados de las auditorias sean informados a la dirección pertinente; y
g) conservar la información documentada como evidencia del programa de auditoría y los resultados de la auditoría.

9.3 Revisión por la dirección

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados para garantizar su conveniencia, suficiencia y eficacia.

La revisión por la dirección debe incluir la consideración de:

a) el estado de las acciones de revisiones previas por la dirección:
b) los cambios en los asuntos externos e internos que son pertinentes para el sistema de gestión de la seguridad de la información;
c) la retroalimentación sobre el desempeño de la seguridad de la información, incluyendo a las tendencias en:
    1) las no conformidades y las acciones correctivas;
    2) los resultados del seguimiento y la medición;
    3) los resultados de la auditoría; y
    4) el cumplimiento de los objetivos de seguridad de la información;
d) retroalimentación de las partes interesadas;
e) resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos; y
f) oportunidades para la mejora continua.

Los resultados de la revisión por la dirección deben incluir a las decisiones realizadas con las oportunidades de mejora continua y cualquier necesidad de cambios para el sistema de gestión de la seguridad de la información.

La organización debe conservar l información documentada como evidencia de los resultados de las revisiones por la dirección.

10. MEJORA

10.1 No conformidades y acciones correctivas

Cuando se produce una no conformidad, la organización debe:

a) reaccionar a la no conformidad, y, según corresponda:

1) adoptar medidas para controlar y corregirla; y
2) hacer frente a las consecuencias;

b) evaluar la necesidad de adaptar medidas para eliminar las causas de las no conformidades a fin de que no se repita u ocurra en otros lugares:
1) revisando la no conformidad;
2) determinando las causas de la no conformidad; y
3) determinando si existen o podrían ocurrir no conformidades similares;

c) implantar las medidas oportunas;
d) revisar la eficacia de las acciones correctivas adoptadas; y
e) realizar cambios al sistema de gestión de la seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe conservar la información documentada como evidencia de:

f) la naturaleza de las no conformidades y de cualquier acción adoptada posteriormente y
g) los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la conveniencia, suficiencia y eficacia del sistema de gestión de la seguridad de la información.

ANEXO A

(Normativo)

OBJETIVOS DE CONTROL DE REFERENCIA Y CONTROLES

Los objetivos de control y los controles indicados en la tabla A.1 se derivan directamente de y se alinean con los listados en la Norma ISO/IEC 27002 Capítulo 5 al 18 y se van a utilizar en el contexto del apartado 6.1.3.

Tabla A.1 - Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Orientación de la dirección para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y leyes pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* La dirección debe definir y aprobar un conjunto de políticas para la seguridad de la información y éstas se deben publicar y comunicar a todos los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información debe ser revisadas a intervalos planificados o si ocurren cambios significativos para garantizar su continua conveniencia, suficiencia y eficacia.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		

A.6.1.1	Funciones y responsabilidades de seguridad de la información	*Control* Todas las responsabilidades deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	*Control* Las funciones en conflicto y las áreas de responsabilidad deben ser segregadas para reducir las oportunidades de modificación no autorizada, no intencional o por mal uso de los activos de la organización.
A.6.1.3	Contacto con autoridades	*Control* Deben mantenerse contactos apropiados con las autoridades relevantes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Deben mantenerse los contactos apropiados con los grupos de interés especial u otros foros especializados en seguridad, así como asociaciones de profesionales.
A.6.1.5	Seguridad de la información en gestión de proyectos *** (VER LA NOTA 1)**	*Control* La seguridad de la información debe ser abordada en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2 Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
A.6.2.1	Política de dispositivos móviles	*Control* Debe adoptarse una política y medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles
A.6.2.2	Teletrabajo	*Control* Debe implantarse una política y medidas de seguridad de apoyo para proteger la información accedida, procesada o almacenada en sitios de teletrabajo.
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
A.7.1.1	Selección	*Control* Debe realizarse la verificación de antecedentes del empleo de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.
*** NOTA 1:** Para profundizar en el concepto de abordaje de la seguridad de la información en la gestión de proyectos véase el apartado 6.1.5 de la Norma ISO/IEC 27002:2013		
A.7.1.2	Términos y condiciones de la relación laboral	*Control* Los acuerdos contractuales con los empleados y contratistas deben iniciar sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con las responsabilidades de		

seguridad de la información.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a los empleados y contratistas aplicar la seguridad de acuerdo con las políticas y los procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y formación en seguridad de la información	*Control* Todos los empleados de la organización y cuando sea pertinente, los contratistas deben recibir una educación adecuada en concientización y formación y actualización y regulares en políticas y procedimientos organizacionales, relevantes para su función laboral.
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal y comunicado para adoptar medidas contra los empleados que han perpetrado una violación a la seguridad.
A.7.3 Finalización y cambio de la relación laboral o empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambiar o finalizar la relación laboral.		
A.7.3.1	Finalización o cambio de responsabilidades laborales	*Control* Las responsabilidades y las funciones de la seguridad de la información que siguen vigentes luego de la finalización o el cambio de la relación laboral o empleo deben ser definidas, comunicadas al empleado o contratista y obligatorias.
A.8 Gestión de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	*Control* Deben ser identificados los activos asociados con los recursos de procesamiento de información y con la información y se debe establecer y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben contar con un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Deben identificarse, documentarse e implantarse las reglas para el uso aceptable de la información y los activos asociados con la información y con las instalaciones de procesamiento de información.
A.8.1.4	Devolución de los activos	*Control* Todos los empleados y los usuarios de partes externas deben devolver todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.		

A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en función de los requisitos legales, del valor, de la criticidad y de la sensibilidad a la divulgación no autorizada o la modificación.
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información, adoptado por la organización.
A.8.2.3	Gestión de activos	*Control* Procedimientos para la gestión de activos deben ser desarrollados e implantados de acuerdo con el esquema de la clasificación de la información adoptado por la organización.
A.8.3 Manejo de medios		
Objetivo: Prevenir la divulgación no autorizada, la modificación, la eliminación o la destrucción de la información almacenadas en los medios.		
A.8.3.1	Gestión de los medios removibles	*Control* Deben implantarse procedimientos para la gestión de los medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	*Control* Los medios deben ser dispuestos cuando ya no son necesarios, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de negocios del control de acceso		
Objetivo: Limitar el acceso a la información y a las instalaciones de procedimientos de información		
A.9.1.1	Política de control de acceso	*Control* Una política de control de acceso debe ser establecida, documentada y revisada en base a los requisitos de negocios y de la seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	*Control* Los usuarios sólo deben disponer de acceso a las redes y a los servicios de red a los que han sido autorizados específicamente para su uso.
A.9.2 Gestión de acceso del usuario		
Objetivo: Garantizar el acceso autorizado a los usuarios y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuarios	*Control* Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.

A.9.2.2	Previsión de accesos a los usuarios	*Control* Debe implementarse un proceso de provisión de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control* La asignación y la utilización de los derechos de acceso privilegiados deben ser restringidas y controladas.
A.9.2.4	Gestión de información de autenticación secreta de los usuarios	*Control* La asignación de información de autenticación secreta debe ser controlada a través de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos planificados.
A.9.2.6	Remoción o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de los usuarios externos a la información y a las instalaciones de procesamiento de la información deben ser removidos luego de la finalización del empleo, contrato o acuerdo, o ser ajustado al cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información de autenticación secreta	*Control* Los usuarios deben seguir las prácticas de la organización en el uso de la información de autenticación secreta.
A.9.4 Control de acceso del sistema y la aplicación		
Objetivo: Prevenir el acceso no autorizado a los sistemas y las aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de aplicación del sistema debe ser restringido de acuerdo con la política de control de acceso.
A.9.4.2	Procesamientos seguros de inicio de sección (log on)	*Control* Cuando lo requiera la política de control de acceso, el acceso de los sistemas y aplicaciones debe ser controlado por un procedimiento seguro de inicio de sesión (log on)
A.9.4.3	Sistema de gestión de contraseña	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben garantizar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* El uso de programas utilitarios que podría ser capaz de anular los controles del sistema y de las aplicaciones debe ser restringido y estrechamente controlado.

A.9.4.5	Control de acceso del código fuente del programa	*Control* El acceso al código fuente del programa debe ser restringido.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información.		
A.10.1.1	Política sobre el uso de los controles criptográficos	*Control* Debe desarrollarse e implantarse una política sobre el uso de los controles criptográficos para proteger la información.
A.10.1.2	Gestión de claves	*Control* Debe desarrollarse e implantarse una política sobre el uso, protección y duración de las claves criptográficas a través de todo su ciclo de vida.
A.11 Seguridad física y del ambiente		
A.11.1 Áreas seguras		
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información.		
A.11.1.1	Perímetro de seguridad física	Deben definirse los perímetros de seguridad y ser utilizados para proteger las áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras deben estar protegidas por controles de entrada apropiadas que aseguren que sólo se permite el acceso de personal autorizado.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones	*Control* Debe diseñarse y aplicarse seguridad física a oficinas, despachos e instalaciones.
A.11.1.4	Protección contra amenazas externas y del ambiente	*Control* Debe diseñarse y aplicarse protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	El trabajo en las áreas seguras	*Control* Deben diseñarse y aplicarse procedimientos para trabajar en áreas seguras.
A.11.1.6	Áreas de entrega y de carga	*Control* Los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones debe ser controlado y, si es posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2 Equipamiento		
Objetivo: Prevenir pérdidas, daños, hurtos o comprometer los activos, así como la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	*Control* El equipamiento debe estar ubicado y ser

		protegido para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
A.11.2.2	Servicios de apoyo	*Control* Debe protegerse el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causadas por fallas en los servicios de apoyo
A.11.2.3	Seguridad en el cableado	*Control* El cableado de energía y de telecomunicaciones que transportan datos o servicios de información de apoyo debe ser protegido de la intercepción, la interferencia o los daños.
A.11.2.4	Mantenimiento del equipamiento	*Control* El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.
A.11.2.5	Remoción de los activos	*Control* Los equipamientos, la información o el software no se deben sacar fuera de las instalaciones de la organización sin autorización previa.
A.11.2.6	Seguridad del equipamiento y de los archivos fuera de las instalaciones de la organización	*Control* Deben asegurarse todos los activos fuera de los locales de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Seguridad en la reutilización o eliminación de los equipos	*Control* Todo aquel equipamiento que contenga medios de almacenamiento deben revisarse para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su disposición o reutilización.
A.11.12.8	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección adecuada.
A.11.2.9	Política de escritorio y pantalla limpios	*Control* Debe adoptarse una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones		
A.12.1 Procesamientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.		
A.12.1.1	Procesamientos documentados de operación	*Control* Los procesamientos de operación deben documentarse, mantenerse y ponerse a

		disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Los cambios en la organización, los procesos del negocio, las instalaciones de procesamiento de información y los sistemas que afectan la seguridad de la información, deben ser controlados.
A.12.1.3	Gestión de la capacidad	*Control* Debe supervisarse y adaptarse el uso de recursos, así como proyecciones de los frutos requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los recursos para desarrollo, prueba y ambientes operacionales	*Control* Los recursos para el desarrollo, prueba y ambientes operacionales deben separase para reducir los riesgos de acceso no autorizado o los cambios en el ambiente operacionales.
A.12.2 Protección contra el *malware*		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el *malware.*		
A.12.2.1	Controles contra el *malware*	*Control* Los controles de detección, prevención, y recuperación para proteger contra el *malware* deben ser implementados, combinados con el conocimiento correspondiente del usuario.
A.12.3 Respaldo		
Objetivo: Protección contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Deben hacerse regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo.
A.12.4 Registro y seguimiento		
Objetivo: Registrar los eventos y generar evidencia.		
A.12.4.1	Registros de eventos	*Control* Los registros de eventos que registran actividades del usuario, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y revisados regularmente.
A.12.4.2	Protección de la información de registros (logs)	*Control* Los medios de registro y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar y los registros deben ser protegidos y revisados regularmente.
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinente

		dentro de una organización o domino de seguridad deben estar sincronizados a una sola fuente de referencia de tiempo.
A.12.5 Control del software en producción		
Objetivo: Garantizar la integridad de los sistemas operativos.		
A.12.5.1	Instalación de software en los sistemas operativos	*Control* Deben implantarse procedimientos para controlar la instalación de software en los sistemas operativos
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Evitar la explotación de vulnerabilidades técnicas.		
A.12.6.1	Gestión de vulnerabilidades técnicas	*Control* Debe obtenerse información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información, debe evaluarse la exposición de la organización a estas vulnerabilidades, y deben tomarse las medidas apropiadas para abordar el riesgo asociado.
A.12.6.2	Restricciones a la instalación de software	*Control* Deben establecerse e implantarse reglas relativas a la instalación de software por los usuarios.
A.12.7 Consideraciones de la auditoría de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que implican la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de seguridad de la red		
Objetivo: Garantizar la protección de la información en las redes y en sus recursos de procesamiento de información de apoyo.		
A.13.1.1	Controles de la red	*Control* Deben gestionarse y controlarse las redes para proteger la información en los sistemas y las aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en los acuerdos de servicios de red, ya sea que estos servicios sean prestados en la empresa o subcontratados.
A.13.1.3	Segregación en las redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información deben ser segregados en las redes.
A.13.2 Transferencia de información		

Objetivo: Mantener la seguridad de la información transferencia dentro de la organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Deben establecerse políticas, procedimientos y controles formales de transferencia, para proteger la transferencia de información
A.13.2.2	Acuerdos sobre la transferencia de información	*Control* Los acuerdos deben abordar la transferencia de información comercial entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* La información involucrada en la mensajería electrónica se debe proteger apropiadamente.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Deben identificarse, revisarse regularmente y documentarse los requisitos sobre acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información, a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información se deben incluir en los requisitos para los nuevos sistemas de información existentes.
A.14.1.2	Servicios de aplicación de seguridad en las redes públicas	*Control* La información implicada en los servicios de aplicación que pasa a través de las redes públicas debe estar protegida contra la actividad fraudulenta, la disputa contractual y la divulgación y modificación no autorizada.
A.14.1.3	Transacciones de protección de los servicios de aplicación	*Control* La información implicada en las transacciones de los servicios de aplicación debe estar protegida para prevenir la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.
A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Garantizar que la seguridad de la información se ha diseñado e implementado en el ciclo de vida del desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control*

		Deben establecerse y aplicarse reglas para el desarrollo de software y sistemas dentro de la organización.
A.14.2.2	Procedimientos de control de cambios del sistema	*Control* Los cambios en los sistemas dentro del ciclo de vida de desarrollo se deben controlar por el uso de procedimientos de control de cambios formales.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	*Control* Cuando las plataformas operativas cambian, las aplicaciones críticas del negocio se deben revisar y poner a prueba para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Debe desalentarse la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de la ingeniería de sistemas segura	*Control* Los principios de la ingeniería de sistemas segura deben ser establecidos, documentados, mantenidos y aplicados a los esfuerzos de implementación de cualquier sistema de información.
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para los esfuerzos de desarrollo e integración de sistemas, que cubren todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Desarrollo subcontratado	*Control* La organización debe supervisar y realizar el seguimiento de las actividades de desarrollo de sistemas subcontratadas.
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Deben llevarse a cabo pruebas de las funcionalidades de seguridad, durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	*Control* Deben establecerse programas de pruebas de aceptación y los criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Garantizar la protección de los datos utilizados para la prueba.		
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		

Objetivo: Garantizar la protección de los activos de la organización, accesibles por los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	*Control* Los requisitos de seguridad de información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben ser acodados con el proveedor y documentados.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con los proveedores	*Control* Todos los requisitos pertinentes se seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de las tecnologías de la información y las comunicaciones	*Control* Los acuerdos con los proveedores deben incluir requisitos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de información y de servicios y productos de tecnologías de las comunicaciones.
A.15.2 Gestión de la prestación de servicios del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y de la presentación de servicios en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben realizar el seguimiento, revisar y auditar regularmente la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Los cambios en la presentación de servicios de los proveedores, incluyendo el mantenimiento y mejora de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocios involucrados y reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras de seguridad de la información		
Objetivo: Garantizar un enfoque coherente y eficaz a la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.		
A 16.1.1	Responsabilidades y procedimientos	*Control* Deben establecerse responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.
A 16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben reportar a través de los canales de gestión apropiados, lo más rápidamente

		posible.
A 16.1.3	Reporte de las debilidades de seguridad de la información	*Control* Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización, deben observar y reportar cualquier debilidad en la seguridad de sistemas o servicios, observada o que se sospeche.
A 16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser evaluados y se debe decidir si son clasificados como incidentes de seguridad de la información.
A 16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A 16.1.6	Aprender de los incidentes de seguridad de la información	*Control* Los conocimientos adquiridos en el análisis y la resolución de los incidentes de seguridad de la información deben ser utilizados para reducir la probabilidad o el impacto de futuros incidentes.
A 16.1.7	Recopilación de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y conservación, de información, que puede servir como evidencia.
A. 17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A. 17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe ser incluida en los sistemas de gestión de continuidad del negocio de la organización.		
A 17.1.1	Planificación de la continuidad de la seguridad de la información	Control La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A 17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implantar y mantener procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.
A 17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	*Control* La organización debe verificar los controles establecidos e implementados de la continuidad de la seguridad de la información a intervalos regulares, con el fin de asegurar que sean válidas y efectivas

		en situaciones adversas.
A 17.2 Redundancia		
Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de información.		
A 17.2.1	Disponibilidad de las instalaciones de procesamiento de información	*Control* Deben implantarse las instalaciones de procesamiento de información con la suficiente redundancia como para cumplir los requisitos de disponibilidad.
A 18 Cumplimiento		
A 18.1 Cumplimiento con los requisitos legales y contractuales		
A 18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Control Todos los requisitos legislativos, estatutarios, reglamentarios, contractuales y el enfoque de la organización para cumplirlos debe ser explícitamente definidos, documentados y actualizados para cada sistema de información y para la organización.
A 18.1.2	Derechos de propiedad intelectual	Control Deben implantarse procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A 18.1.3	Protección de los registros	Control Los registros se deben proteger contra pérdida, destrucción, falsificación
A 18.1.4		
A 18.1.5		
A 18.2 Revisiones de seguridad de la información		
Objetivo: Garantizar que la seguridad de la información sea implementada y que funciona de acuerdo con las políticas y procedimientos de la organización		
A 18.2.1	Revisión independiente de seguridad de la información	*Control* El enfoque de la organización para gestionar seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deben ser revisados independientemente a intervalos planificados o cuando se produzcan otros cambios significativos.
A 18.2.2	Conformidad con las políticas y normas de seguridad	*Control* Los directivos deben revisar regularmente la conformidad con el procesamiento y los procedimientos de información, dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad adecuados.
A 18.2.3	Revisión de conformidad técnica	*Control* Los sistemas de información deben ser

		revisados regularmente por su conformidad con las políticas y las normas de seguridad de la información de la organización.