ESTÁNDAR
ISO / IEC 27001

Segunda edicion
2013-10-01
Número de referencia
ISO / IEC 27001: 2013 (E)

DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR

Oficina de derechos de autor ISO
Caso postale 56 • CH-1211 Ginebra 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
Correo electrónico copyright@iso.org
Web www.iso.org
Publicado en Suiza

Contenido

Página

ISO / IEC 27001: 2013 (E)

Prefacio

ISO (la Organización Internacional de Normalización) e IEC (la Internacional Electrotécnica Comisión) forman el sistema especializado para la estandarización mundial. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de estándares internacionales a través de técnicas comités establecidos por la organización respectiva para ocuparse de campos técnicos particulares actividad. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otro internacional organizaciones, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO / IEC JTC 1.

Las Normas Internacionales están redactadas de acuerdo con las reglas dadas en las Directivas ISO / IEC, Parte 2. La tarea principal del comité técnico conjunto es preparar Normas Internacionales. Draft International Las normas adoptadas por el comité técnico conjunto se distribuyen a los organismos nacionales para su votación. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos nacionales. emitir un voto

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no serán responsables de identificar ninguno o todos los derechos de patente.

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

Esta segunda edición cancela y reemplaza la primera edición (ISO / IEC 27001: 2005), que ha sido revisado técnicamente

ISO / IEC 27001: 2013 (E)

0 Introducción

0.1 General

Esta Norma Internacional ha sido preparada para proporcionar requisitos para establecer, implementar, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información. La adopción de un El sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento y la implementación del sistema de gestión de seguridad de la información de una organización está influenciada por necesidades y objetivos de la organización, requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad. de información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de seguridad de la información forme parte de e integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considera en el diseño de procesos, sistemas de información y controles. Se espera que una seguridad de la información La implementación del sistema de gestión se ampliará de acuerdo con las necesidades de la organización.

Esta norma internacional puede ser utilizada por partes internas y externas para evaluar la organización capacidad para cumplir con los requisitos de seguridad de la información propios de la organización.

El orden en que se presentan los requisitos en esta Norma Internacional no refleja su importancia o implica el orden en que se implementarán. Los elementos de la lista se enumeran para Propósito de referencia solamente.

ISO / IEC 27000 describe la descripción general y el vocabulario de la gestión de seguridad de la información sistemas, haciendo referencia a la familia de estándares del sistema de gestión de seguridad de la información (incluidos ISO / IEC 27003 [2] , ISO / IEC 27004 [3] e ISO / IEC 27005 [4]), con términos y definiciones relacionados.

0.2 Compatibilidad con otros estándares del sistema de gestión

Esta norma internacional aplica la estructura de alto nivel, títulos de subcláusula idénticos, texto idéntico, términos comunes y definiciones básicas definidas en el Anexo SL de las Directivas ISO / IEC, Parte 1, ISO consolidado Complementa y, por lo tanto, mantiene la compatibilidad con otros estándares del sistema de gestión que tienen adoptó el anexo SL.

Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que eligen operar Un sistema de gestión único que cumple con los requisitos de dos o más estándares del sistema de gestión.

Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos

1 Alcance

Esta Norma Internacional especifica los requisitos para establecer, implementar y mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de organización. Esta Norma Internacional también incluye requisitos para la evaluación y el tratamiento. de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en este Norma Internacional son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de de tipo, tamaño o naturaleza. Excluir cualquiera de los requisitos especificados en las Cláusulas 4 a 10 no es aceptable cuando una organización declara conformidad con esta Norma Internacional.

2 Referencias normativas

Los siguientes documentos, en su totalidad o en parte, están referenciados normativamente en este documento y son indispensable para su aplicación. Para las referencias con fecha, sólo se aplica la edición citada. Para sin fecha referencias, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO / IEC 27000, *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información sistemas - Resumen y vocabulario*

3 Términos y definiciones

Para los propósitos de este documento, se aplican los términos y definiciones dados en ISO / IEC 27000.

4 Contexto de la organización

4.1 Comprensión de la organización y su contexto.

La organización debe determinar los problemas externos e internos que son relevantes para su propósito y que afectar su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.

NOTA

La determinación de estos problemas se refiere al establecimiento del contexto externo e interno de la organización. considerado en la Cláusula 5.3 de ISO 31000: 2009 [5] .

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) partes interesadas que son relevantes para el sistema de gestión de seguridad de la información; y

b) los requisitos de estas partes interesadas relevantes para 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 seguridad de la información

La organización debe determinar los límites y la aplicabilidad de la seguridad de la información.

sistema de gestión 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 4.2; y

c) interfaces y dependencias entre las actividades realizadas por la organización y aquellas que son realizado por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de la información.

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

5 liderazgo

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto a la información. sistema de gestión de seguridad por:

a) garantizar la política de seguridad de la información y los objetivos de seguridad de la información establecidos y son compatibles con la dirección estratégica de la organización;

b) asegurar la integración de los requisitos del sistema de gestión de seguridad de la información en el procesos de la organización;

c) asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;

d) comunicar la importancia de una gestión eficaz de la seguridad de la información y de cumplir con los requisitos del sistema de gestión de seguridad de la información;

e) asegurar que el sistema de gestión de seguridad de la información logre los resultados previstos;

f) dirigir y apoyar a las personas para que contribuyan a la efectividad de la seguridad de la información sistema de gestión;

g) promover la mejora continua; y

h) respaldar otras funciones de gestión relevantes para demostrar su liderazgo tal como se aplica a sus Areas de responsabilidad.

5.2 Política

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

a) es apropiado para el propósito de la organización;

b) incluye objetivos de seguridad de la información (ver 6.2) o proporciona el marco para establecer información objetivos de seguridad;

c) incluye un compromiso para satisfacer los requisitos aplicables relacionados con la seguridad de la información; y

d) incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información deberá:

e) estar disponible como información documentada;

f) ser comunicados dentro de la organización; y

g) estar disponible para las partes interesadas, según corresponda.

5.3 Roles organizacionales, responsabilidades y autoridades

La alta dirección debe garantizar que las responsabilidades y autoridades para los roles relevantes para la información
Se asignan y comunican seguridad.
La alta dirección debe asignar la responsabilidad y la autoridad para:
a) asegurar que el sistema de gestión de seguridad de la información se ajuste a los requisitos de este
Estándar internacional; y
b) informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.
NOTA
La alta gerencia también puede asignar responsabilidades y autoridades para informar el desempeño de la
sistema de gestión de seguridad de la información dentro de la organización.

6 planificación

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 General

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar
cuestiones mencionadas en 4.1 y los requisitos mencionados en4.2 y determinar los riesgos y oportunidades
que deben dirigirse a:
a) garantizar que el sistema de gestión de la seguridad de la información pueda lograr los resultados previstos;
b) prevenir o reducir los efectos no deseados; y
c) lograr la mejora continua.
La organización debe planificar:
d) acciones para abordar estos riesgos y oportunidades; y
e) cómo
1) integrar e implementar las acciones en su sistema de gestión de seguridad de la información
procesos; 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) establece y mantiene criterios de riesgo de seguridad de la información que incluyen:
1) los criterios de aceptación del riesgo; y
2) criterios para realizar evaluaciones de riesgos de seguridad de la información;
b) asegura que las evaluaciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y
resultados comparables;

c) identifica los riesgos de seguridad de la información:
1) aplique el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance de la información
sistema de gestión de seguridad; y
2) identificar a los propietarios del riesgo;
d) analiza los riesgos de seguridad de la información:
1) evaluar las posibles consecuencias que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran
materializar
2) evaluar la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y
3) determinar los niveles de riesgo;
e) evalúa los riesgos de seguridad de la información:
1) compare los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a); y
2) priorizar los riesgos analizados para el tratamiento del riesgo.
La organización debe retener información documentada sobre el riesgo de seguridad de la información.
proceso de evaluacion.

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 opciones apropiadas de tratamiento de riesgos de seguridad de la información, teniendo en cuenta el riesgo

resultados de la evaluación;
b) determinar todos los controles necesarios para implementar el tratamiento de riesgos de seguridad de la información opción (s) elegida (s);
NOTA
Las organizaciones pueden diseñar controles según sea necesario, o identificarlos desde cualquier fuente.
c) compare los controles determinados en 6.1.3 b) arriba con aquellos enAnexo A y verifique que no sea necesario los controles han sido omitidos;
NOTA 1 El Anexo A contiene una lista completa de objetivos y controles de control. Usuarios de esta Internacional Las normas se dirigen al Anexo A para garantizar que no se pasen por alto los controles necesarios.
NOTA 2 Los objetivos de control están implícitamente incluidos en los controles elegidos. Los objetivos de control y Los controles enumerados en el Anexo A no son exhaustivos y pueden ser necesarios objetivos y controles de control adicionales.
d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) yc)) y justificación de inclusiones, ya sea que se implementen o no, y la justificación de exclusiones de 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 la aceptación del riesgos residuales de seguridad de la información.
La organización debe retener información documentada sobre el tratamiento del riesgo de seguridad de la información. proceso.
NOTA
El proceso de evaluación y tratamiento de riesgos de seguridad de la información en esta Norma Internacional se alinea con los principios y lineamientos genéricos provistos en ISO 31000 [5] .

6.2 Objetivos de seguridad de la información y planificación para alcanzarlos

La organización debe establecer objetivos de seguridad de la información en las funciones y niveles relevantes.
Los objetivos de seguridad de la información deberán:
a) ser coherente con la política de seguridad de la información;
b) ser medible (si es posible);
c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación de riesgos y tratamiento de riesgo;
d) ser comunicado; y
e) ser actualizado según corresponda.
La organización debe retener información documentada sobre los objetivos de seguridad de la información.
Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:
f) lo que se hará;
g) qué recursos se requerirán;
h) quién será responsable;
i) cuándo se completará; y
j) cómo se evaluarán los resultados.

7 soporte

7.1 Recursos

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

7.2 Competencia

La organización debe:
a) determinar la competencia necesaria de la persona (s) que realiza el trabajo bajo su control que afecta su desempeño de seguridad de la información;
b) asegurar que estas personas sean competentes sobre la base de una educación, capacitación o experiencia apropiadas;
c) cuando corresponda, tomar medidas para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y

d) retener información documentada apropiada como evidencia de competencia.
NOTA
Las acciones aplicables pueden incluir, por ejemplo: la provisión de capacitación a, la tutoría o la recuperación
asignación de empleados actuales; o la contratación o contratación de personas competentes.

7.3 Conciencia

Las personas que trabajen bajo el control de la organización deben tener en cuenta:
a) la política de seguridad de la información;

b) su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo
los beneficios de mejorar el rendimiento de la seguridad de la información; y
c) las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes para el
sistema de gestión de seguridad de la información que incluye:
a) sobre qué comunicar;
b) cuándo comunicarse;
c) con quién comunicarse;
d) quién se comunicará; y
e) los procesos por los cuales se efectuará la comunicación.

7.5 Información documentada

7.5.1 General

El sistema de gestión de seguridad de la información de la organización debe incluir:
a) información documentada requerida por esta Norma Internacional; y
b) información documentada determinada por la organización como necesaria para la efectividad de
El sistema de gestión de seguridad de la información.
NOTA
El alcance de la información documentada para un sistema de gestión de seguridad de la información puede diferir
de una organización a otra debido a:
1) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;
2) la complejidad de los procesos y sus interacciones; y
3) la competencia de las personas.

7.5.2 Crear y actualizar

Al crear y actualizar la información documentada, la organización debe garantizar lo apropiado:
a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);
b) formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico); y
c) revisión y aprobación de idoneidad y adecuación.

7.5.3 Control de información documentada

Información documentada requerida por el sistema de gestión de seguridad de la información y por este
Norma Internacional se controlará para garantizar:
a) está disponible y es adecuado para su uso, donde y cuando sea necesario; y
b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

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

c) distribución, acceso, recuperación y uso;
d) almacenamiento y preservación, incluida la preservación de la legibilidad;
e) control de cambios (por ejemplo, control de versiones); y
f) retención y disposición.
Información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, se identificarán como apropiado y controlado.
NOTA
El acceso implica una decisión con respecto al permiso para ver solo la información documentada, o el permiso y autoridad para ver y cambiar la información documentada, etc.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con la seguridad de la información.
requisitos, y para implementar las acciones determinadas en 6.1 . La organización también debe implementar planea alcanzar los objetivos de seguridad de la información determinados en 6.2 .
La organización debe mantener información documentada en la medida necesaria para tener la confianza de que Los procesos se han llevado a cabo según lo previsto.
La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados. tomar medidas para mitigar cualquier efecto adverso, según sea necesario.
La organización debe garantizar que los procesos tercerizados se determinen y controlen.

8.2 Evaluación de riesgos de seguridad de la información

La organización debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen u ocurren cambios significativos, teniendo en cuenta los criterios establecidos en 6.1.2 a).
La organización debe retener información documentada de los resultados de la seguridad de la información. evaluaciones de riesgo.

8.3 Tratamiento de riesgos de seguridad de la información

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.
La organización debe retener información documentada de los resultados de la seguridad de la información. tratamiento de riesgo.

9 Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación.

La organización debe evaluar el desempeño de la seguridad de la información y la efectividad de sistema de gestión de seguridad de la información.
La organización debe determinar:
a) lo que necesita ser monitoreado y medido, incluidos los procesos y controles de seguridad de la información;

b) los métodos de monitoreo, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos;
NOTA
Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos.
c) cuándo se realizarán el monitoreo y la medición;
d) quién supervisará y medirá;
e) cuándo se analizarán y evaluarán los resultados del monitoreo y la medición; y
f) quién analizará y evaluará estos resultados.
La organización debe retener información documentada apropiada como evidencia del monitoreo y resultados de la medición.

9.2 Auditoría interna

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si El sistema de gestión de seguridad de la información:

a) se ajusta a
1) los requisitos propios de la organización para su sistema de gestión de seguridad de la información; y
2) los requisitos de esta Norma Internacional;
b) se implementa y mantiene de manera efectiva.
La organización debe:
c) planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluida la frecuencia, los métodos, responsabilidades, requisitos de planificación e informes. Los programas de auditoría deberán tener en cuenta consideración de la importancia de los procesos involucrados y los resultados de auditorías previas;
d) definir los criterios de auditoría y el alcance de cada auditoría;
e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;
f) garantizar que los resultados de las auditorías se comuniquen a la dirección pertinente; y
g) retener información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.

9.3 Revisión de la gerencia

La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización en la fecha prevista intervalos para garantizar su idoneidad, adecuación y eficacia continuas.
La revisión de la dirección incluirá la consideración de:
a) el estado de las acciones de revisiones administrativas anteriores;
b) cambios en los problemas externos e internos que son relevantes para la gestión de la seguridad de la información sistema;
c) comentarios sobre el rendimiento de la seguridad de la información, incluidas las tendencias en:
1) no conformidades y acciones correctivas;
2) resultados de monitoreo y medición;
3) resultados de la auditoría; y

4) cumplimiento de los objetivos de seguridad de la información;
d) comentarios de las partes interesadas;
e) resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos; y
f) oportunidades de mejora continua.
Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con la mejora continua oportunidades y cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.
La organización debe retener información documentada como evidencia de los resultados de las revisiones de la gerencia.

10 mejora

10.1 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:
a) reaccionar ante la no conformidad, y según corresponda:
1) tomar medidas para controlarlo y corregirlo; y
2) lidiar con las consecuencias;
b) evaluar la necesidad de actuar para eliminar las causas de la no conformidad, a fin de que no se repita o ocurrir en otro lugar, por:
1) revisión de la no conformidad;
2) determinar las causas de la no conformidad; y
3) determinar si existen no conformidades similares, o podrían ocurrir potencialmente;
c) implementar cualquier acción necesaria;
d) revisar la efectividad de cualquier acción correctiva tomada; y
e) realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.
Las acciones correctivas serán apropiadas a los efectos de las no conformidades encontradas.
La organización debe retener información documentada como evidencia de:
f) la naturaleza de las no conformidades y cualquier acción posterior tomada, y
g) los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y efectividad de la información.

sistema de gestión de seguridad.

Anexo A
(normativo)
Objetivos de control de referencia y controles

Los objetivos de control y controles enumerados en La tabla A.1 se deriva directamente y se alinea con las enumerados en ISO / IEC 27002: 2013 [1] , Cláusulas 5 a 18 y deben usarse en contexto conCláusula 6.1.3 .

Tabla A.1 - Objetivos de control y controles

A.5 Políticas de seguridad de la información.

A.5.1 Dirección de gestión para la seguridad de la información.

Objetivo: proporcionar dirección de gestión y soporte para la seguridad de la información de acuerdo con requisitos comerciales y leyes y regulaciones relevantes.

A.5.1.1
Políticas de información
seguridad de la nación
Controlar
Se definirá, aprobará un conjunto de políticas para la seguridad de la información.
por la gerencia, publicado y comunicado a los empleados y
partes externas relevantes.

A.5.1.2
Revisión de la política
pide información
seguridad
Controlar
Las políticas de seguridad de la información se revisarán en la fecha prevista.
intervalos o si ocurren cambios significativos para asegurar su continuidad
idoneidad, adecuación y efectividad.

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 operación de seguridad de la información dentro de la organización.

A.6.1.1
Seguridad de información
roles y responsabilidades
corbatas
Controlar
Todas las responsabilidades de seguridad de la información se definirán y asignarán
cated.

A.6.1.2.
Segregación de deberes
Controlar
Deberes y áreas de responsabilidad en conflicto se segregarán a
reducir las oportunidades para modificaciones no autorizadas o involuntarias
ción o mal uso de los activos de la organización.

A.6.1.3
Contacto con autori-
corbatas
Controlar
Se mantendrán contactos apropiados con las autoridades pertinentes.

A.6.1.4
Contacto con especial
grupos de interes
Controlar
Contactos apropiados con grupos de intereses especiales u otros
Los foros de seguridad y las asociaciones profesionales serán los principales
Tained.
A.6.1.5
Seguridad de información
en *control de* gestión de proyectos
La seguridad de la información se abordará en la gestión del proyecto.
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
Controlar
Se adoptará una política y medidas de seguridad de apoyo para
gestionar los riesgos introducidos mediante el uso de dispositivos móviles.
A.6.2.2
Teletrabajo
Controlar
Se implementará una política y medidas de seguridad de apoyo para
proteger la información accedida, procesada o almacenada en el teletrabajo
sitios.
A.7 Seguridad de recursos humanos
A.7.1 Antes del empleo
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados
capaz para los roles para los que se consideran.
A.7.1.1
Cribado
Controlar
Verificación de antecedentes de todos los candidatos para empleo
se llevará a cabo de conformidad con las leyes y reglamentos pertinentes
y ética y será proporcional a los requisitos comerciales,
la clasificación de la información a acceder y el
riesgos percibidos.
A.7.1.2
Términos y Condiciones
De empleo
Controlar
Los acuerdos contractuales con empleados y contratistas deberán
declarar sus responsabilidades y las de la organización para la información
seguridad.
A.7.2 Durante el empleo
Objetivo: garantizar que los empleados y contratistas conozcan y cumplan con la seguridad de su información
responsabilidades.
A.7.2.1
Responsabilidad de la gerencia
bibilidades

Controlar
La gerencia deberá exigir a todos los empleados y contratistas que soliciten
seguridad de la información de acuerdo con las políticas establecidas
y procedimientos de la organización.
A.7.2.2
Seguridad de información
conciencia, educación
y entrenamiento
Controlar
Todos los empleados de la organización y, cuando corresponda, contrac-
Los tors recibirán una educación y formación de sensibilización adecuadas
y actualizaciones periódicas en las políticas y procedimientos de la organización, como
relevante para su función laboral.
A.7.2.3
Proceso disciplinario
Controlar
Habrá un proceso disciplinario formal y comunicado
en lugar de tomar medidas contra los empleados que han cometido un
violación de seguridad de la información.
A.7.3 Terminación y cambio de empleo
Objetivo: proteger los intereses de la organización como parte del proceso de cambio o finalización
empleo.
A.7.3.1
Terminación o cambio
de respuesta laboral
posibilidades
Controlar
Responsabilidades y deberes de seguridad de la información que siguen siendo válidos
después de la terminación o cambio de empleo se definirá, com
comunicado al empleado o contratista y aplicado.
A.8 Gestión de activos
A.8.1 Responsabilidad por activos
Tabla A.1 *(continuación)*

Objetivo: identificar los activos de la organización y definir las responsabilidades de protección adecuadas.
A.8.1.1
Inventario de activos
Controlar
Activos asociados con la información y el procesamiento de la información.
se identificarán las instalaciones y se hará un inventario de estos activos
ser elaborado y mantenido.
A.8.1.2
Propiedad de los bienes
Controlar
Los bienes mantenidos en el inventario serán de su propiedad.
A.8.1.3
Uso aceptable de
bienes
Controlar
Reglas para el uso aceptable de la información y de los activos asociados.
con la información y las instalaciones de procesamiento de información serán

identificado, documentado e implementado.
A.8.1.4
Devolución de activos
Controlar
Todos los empleados y usuarios externos deberán devolver todos los activos de la organización en su posesión al término de su empleo, contrato o acuerdo.

A.8.2 Clasificación de la información

Objetivo: asegurar 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
mation
Controlar
La información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o modificación.
A.8.2.2
Etiquetado de informa-
ción
Controlar
Se establecerá un conjunto apropiado de procedimientos para el etiquetado de información. desarrollado e implementado de acuerdo con la información esquema de clasificación adoptado por la organización.
A.8.2.3
Manejo de activos
Controlar
Se desarrollarán e implementarán procedimientos para el manejo de activos. mentó de acuerdo con el esquema de clasificación de información adoptado por la organización.

A.8.3 Manejo de medios

Objetivo: evitar la divulgación no autorizada, modificación, eliminación o destrucción de información almacenado en medios.
A.8.3.1
Gestión de remov-
medios capaces
Controlar
Se implementarán procedimientos para la gestión de la remoción medios capaces de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2
Eliminación de medios
Controlar
Los medios deben desecharse de manera segura cuando ya no sean necesarios, utilizando procedimientos formales
A.8.3.3
Transmisiones de medios físicos
fer
Controlar
Los medios que contengan información estarán protegidos contra acceso izado, mal uso o corrupción durante el transporte.

A.9 Control de acceso

A.9.1 Requisitos comerciales de control de acceso

Tabla A.1 *(continuación)*

ISO / IEC 27001: 2013 (E)

Objetivo:
Limitar el acceso a la información y a las instalaciones de procesamiento de información.
A.9.1.1
Política de control de acceso
Controlar
Se establecerá, documentará y establecerá una política de control de acceso.
revisado en función de los requisitos comerciales y de seguridad de la información:
ments.
A.9.1.2
Acceso a las redes
y *control de* servicios de red
Los usuarios solo tendrán acceso a la red y a la red.
servicios de trabajo que han sido autorizados específicamente para usar.

A.9.2 Gestión de acceso de usuarios

Objetivo: garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios
vicios
A.9.2.1
Registro de usuario y
desinscripción
Controlar
Se realizará un proceso formal de registro y cancelación de registro de usuarios.
implementado para permitir la asignación de derechos de acceso.
A.9.2.2
Provisión de acceso de usuario
En g
Controlar
Se implementará un proceso formal de aprovisionamiento de acceso de usuario para
asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y
servicios.
A.9.2.3
Gestión de privi-
derechos de acceso legados
Controlar
La asignación y el uso de los derechos de acceso privilegiado serán
restringido y controlado.
A.9.2.4
Manejo de secreto
información de autenticación
mación de usuarios
Controlar
La asignación de información secreta de autenticación será
controlado a través de un proceso de gestión formal.
A.9.2.5
Revisión del acceso del usuario
derechos
Controlar
Los propietarios de los activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares.
A.9.2.6
Remoción o ajuste
de derechos de acceso
Controlar
Los derechos de acceso de todos los empleados y usuarios externos a
se eliminarán las instalaciones de información y procesamiento de información
tras la terminación de su empleo, contrato o acuerdo, o

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 autenticación secreta
información catiónica
Controlar
Los usuarios deberán seguir las prácticas de la organización en el
uso de información secreta de autenticación.

A.9.4 Sistema y control de acceso a aplicaciones

Objetivo: evitar el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1
Acceso a la información
restricción
Controlar
El acceso a la información y las funciones del sistema de aplicación serán
restringido de acuerdo con la política de control de acceso.

A.9.4.2
Procedimiento de inicio de sesión seguro
dures
Controlar
Donde lo requiera la política de control de acceso, acceso a sistemas y
Las aplicaciones se controlarán mediante un procedimiento de inicio de sesión seguro.

Tabla A.1 *(continuación)*

A.9.4.3
Gestión de contraseña
sistema de ment
Controlar
Los sistemas de gestión de contraseñas serán interactivos y deberán
Garantizar contraseñas de calidad.

A.9.4.4
Uso de utilidades privilegiadas
programas de ity
Controlar
El uso de programas de utilidad que pueden ser capaces de anular
los controles del sistema y de la aplicación deben estar restringidos y estrictamente
revisado.

A.9.4.5
Control de acceso a pro-
código fuente de gramo
Controlar
El acceso al código fuente del programa estará restringido.

A.10 Criptografía

A.10.1 Controles criptográficos

Objetivo: garantizar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad,
ticity y / o integridad de la información.

A.10.1.1
Política sobre el uso de
controles criptográficos *Control*
Una política sobre el uso de controles criptográficos para la protección de

La información debe ser desarrollada e implementada.
A.10.1.2 Gestión de claves
Controlar
Una política sobre el uso, la protección y la vida útil de las claves criptográficas.
se desarrollarán e implementarán a lo largo de todo su ciclo de vida.
A.11 Seguridad física y ambiental.
A.11.1 Áreas seguras
Objetivo: evitar el acceso físico no autorizado, daños e interferencias a la organización
Información y facilidades de procesamiento de información.
A.11.1.1
Seguridad física
perímetro
Controlar
Los perímetros de seguridad se definirán y utilizarán para proteger áreas que
contener información sensible o crítica e información
instalaciones de procesamiento.
A.11.1.2 Controles de entrada física *Control*
Las áreas seguras deben estar protegidas por controles de entrada apropiados para
Asegúrese de que solo el personal autorizado tenga acceso.
A.11.1.3
Asegurar oficinas,
habitaciones e instalaciones
Controlar
Se diseñará la seguridad física para oficinas, habitaciones e instalaciones.
y aplicado
A.11.1.4
Protección contra
externo y ambiental
amenazas mentales
Controlar
Protección física contra desastres naturales, ataques maliciosos o
Los accidentes deben ser diseñados y aplicados.
A.11.1.5
Trabajando en forma segura
áreas
Controlar
Se diseñarán procedimientos para trabajar en áreas seguras y
aplicado.
A.11.1.6
Entrega y carga
áreas
Controlar
Puntos de acceso como áreas de entrega y carga y otros puntos.
donde personas no autorizadas puedan ingresar a las instalaciones
controlado y, si es posible, aislado del procesamiento de información
instalaciones para evitar el acceso no autorizado.
Tabla A.1 *(continuación)*

A.11.2 Equipamiento
Objetivo: evitar pérdidas, daños, robos o compromisos de activos e interrupción de la organización.
operaciones de la nación

A.11.2.1
Ubicación del equipo y
proteccion
Controlar
El equipo debe ubicarse y protegerse para reducir los riesgos de
amenazas y peligros ambientales, y oportunidades para
acceso tornado.
A.11.2.2 Utilidades de soporte
Controlar
El equipo debe estar protegido contra fallas de energía y otros
rupturas causadas por fallas en las utilidades de soporte.
A.11.2.3 Seguridad de cableado
Controlar
Cableado de energía y telecomunicaciones que transporta datos o soporte
Los servicios de información se protegerán de la intercepción.
interferencia o daño.
A.11.2.4
Mantenimiento de equipos
maricón
Controlar
El equipo debe mantenerse correctamente para garantizar su continuidad.
disponibilidad e integridad.
A.11.2.5 Remoción de activos
Controlar
El equipo, la información o el software no se deben llevar fuera del sitio
sin autorización previa
A.11.2.6
Seguridad de los equipos
y activos fuera de prem-
ises
Controlar
La seguridad se aplicará a los activos fuera del sitio teniendo en cuenta la
diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7
Eliminación segura o recuperación
uso de equipo
Controlar
Todos los equipos que contengan medios de almacenamiento deberán ser verificados.
para asegurar que cualquier información confidencial y software con licencia haya sido
eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
A.11.2.8
Usuario desatendido
equipo
Controlar
Los usuarios deben asegurarse de que el equipo desatendido tenga
proteccion.
A.11.2.9
Escritorio claro y claro
política de pantalla
Controlar
Una política de escritorio clara para papeles y medios de almacenamiento extraíbles y
se establecerá una política de pantalla clara para las instalaciones de procesamiento de información
adoptado.

A.12 Seguridad de operaciones

A.12.1 Procedimientos y responsabilidades operacionales

Objetivo: garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

A.12.1.1
Operación documentada

procedimientos
Controlar
Los procedimientos operativos deben documentarse y ponerse a disposición de
Todos los usuarios que los necesitan.
A.12.1.2 Gestión del cambio
Controlar
Cambios en la organización, procesos de negocio, pro- puesta de información.
las instalaciones y sistemas de cesación que afectan la seguridad de la información deberán
ser controlado
Tabla A.1 *(continuación)*

A.12.1.3 *Control de* gestión de capacidad
El uso de los recursos debe ser monitoreado, ajustado y proyecciones
hecho de requisitos de capacidad futuros para garantizar el sistema requerido
rendimiento tem.
A.12.1.4
Separación de desarrollo
opción, prueba y
entorno operacional
ments
Controlar
El desarrollo, las pruebas y los entornos operativos deben estar separados
calificado para reducir los riesgos de acceso no autorizado o cambios en el
entorno operativo.

A.12.2 Protección contra malware

Objetivo: asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra
malware
A.12.2.1
Controles contra mal-
mercancía
Controlar
Detección, prevención y controles de recuperación para proteger contra
se implementará malware, combinado con el usuario apropiado
conciencia.

A.12.3 Copia de seguridad

Objetivo: proteger contra la pérdida de datos.
A.12.3.1 Copia de seguridad de información
Controlar
Se realizarán copias de seguridad de la información, el software y las imágenes del sistema.
tomado y probado regularmente de acuerdo con un respaldo acordado
política.

A.12.4 Registro y monitoreo

Objetivo: registrar eventos y generar evidencia.
A.12.4.1 Registro de eventos
Controlar
Registros de eventos que registran actividades del usuario, excepciones, fallas e información
Los eventos de seguridad de mationes serán producidos, guardados y regularmente
revisados.
A.12.4.2
Protección de información de registro
mation

Controlar
Las instalaciones de registro y la información de registro estarán protegidas contra manipulación y acceso no autorizado.
A.12.4.3
Administrador y
registros de operador
Controlar
Las actividades del administrador del sistema y del operador del sistema serán registrado y los registros protegidos y revisados regularmente.
A.12.4.4 *Control de* sincronización del reloj
Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizará con un
fuente de tiempo de referencia de gle.
A.12.5 Control de software operativo
Objetivo: Asegurar la integridad de los sistemas operativos.
A.12.5.1
Instalación de soft-
Ware en operacional
sistemas
Controlar
Se implementarán procedimientos para controlar la instalación de software Ware en sistemas operativos.
A.12.6 Gestión de vulnerabilidad técnica
Objetivo: evitar la explotación de vulnerabilidades técnicas.
Tabla A.1 *(continuación)*
dieciséis

A.12.6.1
Gestión de tecni-
vulnerabilidades de cal
Controlar
Información sobre vulnerabilidades técnicas de los sistemas de información. siendo utilizado se obtendrá de manera oportuna, la organización
exposición a tales vulnerabilidades evaluadas y medidas apropiadas
ures tomados para abordar el riesgo asociado.
A.12.6.2
Restricciones en soft-
instalación de artículos
Controlar
Las reglas que rigen la instalación de software por parte de los usuarios serán establecido e implementado.
A.12.7 Consideraciones de auditoría de sistemas de información
Objetivo: minimizar el impacto de las actividades de auditoría en los sistemas operativos.
A.12.7.1
Sistemas de información
controles de auditoria
Controlar
Requisitos de auditoría y actividades que implican la verificación de la operación Los sistemas nacionales se planificarán y acordarán cuidadosamente para minimizar interrupciones en los procesos comerciales.
A.13 Seguridad de comunicaciones
A.13.1 Gestión de seguridad de red

Objetivo: Garantizar la protección de la información en las redes y su pro- puesta de información de apoyo.
instalaciones para dejar de fumar.
A.13.1.1 Controles de red
Controlar
Las redes se gestionarán y controlarán para proteger la información.
en sistemas y aplicaciones.
A.13.1.2
Seguridad de la red
servicios
Controlar
Los mecanismos de seguridad, los niveles de servicio y la gestión requieren:
Los elementos de todos los servicios de red se identificarán e incluirán en
acuerdos de servicios de red, si se proporcionan estos servicios
interno o subcontratado.
A.13.1.3
Segregación en red
trabajos
Controlar
Grupos de servicios de información, usuarios y sistemas de información.
se segregará en las redes.

A.13.2 Transferencia de información

Objetivo: mantener la seguridad de la información transferida dentro de una organización y con cualquier
Entidad externa.
A.13.2.1
Transferencia de información
políticas y procedimientos
dures
Controlar
Se deben establecer políticas, procedimientos y controles formales de transferencia.
para proteger la transferencia de información mediante el uso de todo tipo
de instalaciones de comunicación.
A.13.2.2
Acuerdos sobre información
transferencia de mation
Controlar
Los acuerdos abordarán la transferencia segura de información comercial
ción entre la organización y las partes externas.
A.13.2.3 *Control de* mensajes electrónicos
La información involucrada en la mensajería electrónica será apropiada.
Totalmente protegido.

Tabla A.1 *(continuación)*

A.13.2.4
Confidencialidad o no
acuerdos de divulgación
Controlar
Requisitos para acuerdos de confidencialidad o no divulgación
reflejando las necesidades de la organización para la protección de la información
Se identificará, revisará y documentará periódicamente.

A.14 Adquisición, desarrollo y mantenimiento del sistema.

A.14.1 Requisitos de seguridad de los sistemas de información.

Objetivo: garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida completo. Esto también incluye los requisitos para los sistemas de información que prestan servicios. a través de redes públicas.

A.14.1.1
Seguridad de información
análisis de requerimientos
y especificación
Controlar
Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para nuevos sistemas de información o mejoras para sistemas de información existentes.

A.14.1.2
Aplicación de seguridad
servicios en público
redes
Controlar
Información involucrada en los servicios de aplicaciones que pasan por público las redes deben estar protegidas de actividades fraudulentas, contratos deshabilitados divulgación y modificación pute y no autorizada.

A.14.1.3
Aplicación de protección
transacciones de servicios
Controlar
La información involucrada en las transacciones del servicio de aplicación será protegido para evitar transmisiones incompletas, enrutamiento erróneo, alteración de mensajes afectuosa, divulgación no autorizada, no autorizada duplicación o reproducción de mensajes ized.

A.14.2 Seguridad en los procesos de desarrollo y soporte.

Objetivo: garantizar que la seguridad de la información se diseñe e implemente dentro del desarrollo ciclo de vida de los sistemas de información.

A.14.2.1
Desarrollo seguro
política
Controlar
Se establecerán reglas para el desarrollo de software y sistemas. Listed y aplicado a los desarrollos dentro de la organización.

A.14.2.2
Control de cambios del sistema
procedimientos
Controlar
Los cambios en los sistemas dentro del ciclo de vida del desarrollo deberán ser con- controlado por el uso de procedimientos formales de control de cambios.

A.14.2.3
Revisión técnica de
aplicaciones después
plataforma operativa
cambios
Controlar
Cuando se cambian las plataformas operativas, las aplicaciones empresariales críticas Se revisarán y probarán las opciones para garantizar que no haya efectos adversos. impacto en las operaciones organizacionales o la seguridad.

A.14.2.4
Restricciones en
cambios en el software
paquetes
Controlar
Se desaconsejarán las modificaciones a los paquetes de software, limitándose a cambios necesarios y todos los cambios deberán ser estrictamente controlados.

A.14.2.5
Sistema seguro
principios de neering
Controlar
Se establecerán principios para la ingeniería de sistemas seguros.
documentado, mantenido y aplicado a cualquier sistema de información
esfuerzos de implementación.
Tabla A.1 *(continuación)*
18 años

A.14.2.6
Desarrollo seguro
medio ambiente
Controlar
Las organizaciones deben establecer y proteger adecuadamente la seguridad
entornos de desarrollo para desarrollo e integración de sistemas
Esfuerzos que cubren todo el ciclo de vida de desarrollo del sistema.
A.14.2.7
Desarrollo subcontratado
ment
Controlar
La organización debe supervisar y monitorear la actividad de
desarrollo del sistema de origen.
A.14.2.8
Prueba de seguridad del sistema
En g
Controlar
Las pruebas de la funcionalidad de seguridad se llevarán a cabo durante el desarrollo.
Opment.
A.14.2.9
Aceptación del sistema
pruebas
Controlar
Se establecerán programas de prueba de aceptación y criterios relacionados.
En busca de nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba
Objetivo: garantizar la protección de los datos utilizados para las pruebas.
A.14.3.1 Protección de datos de prueba *Control*
Los datos de prueba deben seleccionarse cuidadosamente, protegerse y controlarse.
A.15 Relaciones con proveedores
A.15.1 Seguridad de la información en las relaciones con los proveedores.
Objetivo: Asegurar la protección de los activos de la organización a la que los proveedores puedan acceder.
A.15.1.1
Seguridad de información
política para el proveedor
relaciones
Controlar
Requisitos de seguridad de la información para mitigar los riesgos asociados
El acceso del proveedor a los activos de la organización debe ser
acordado con el proveedor y documentado.
A.15.1.2
Abordar la seguridad

dentro del acuerdo del proveedor
ments
Controlar
Se establecerán todos los requisitos de seguridad de la información relevantes.
y acordado con cada proveedor que pueda acceder, procesar, almacenar,
comunicar o proporcionar componentes de infraestructura de TI para
información de la organización.
A.15.1.3
Información y com
tecnología de comunicación
cadena de suministro
Controlar
Los acuerdos con proveedores incluirán requisitos para abordar
los riesgos de seguridad de la información asociados con la información y
servicios de tecnología de comunicaciones y cadena de suministro de productos.

A.15.2 Gestión de la prestación del servicio del proveedor.

Objetivo: Mantener un nivel acordado de seguridad de la información y prestación de servicios en línea con la asistencia
acuerdos de alicates.
A.15.2.1
Monitoreo y revisión
de servicios de proveedores
Controlar
Las organizaciones deben monitorear, revisar y auditar regularmente al proveedor
prestación de servicios
A.15.2.2
Gestionar cambios a
servicios de proveedores
Controlar
Cambios en la provisión de servicios por parte de proveedores, incluyendo
mantener y mejorar las políticas de seguridad de la información existentes,
los procedimientos y controles, se gestionarán teniendo en cuenta la
criticidad de la información comercial, sistemas y procesos involucrados
y reevaluación de riesgos.

Tabla A.1 *(continuación)*

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes de seguridad de la información y mejoras.

Objetivo: garantizar un enfoque coherente y efectivo para la gestión de la seguridad de la información
incidentes, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1
Responsabilidades y
procedimientos
Controlar
Se establecerán responsabilidades y procedimientos de gestión.
para garantizar una respuesta rápida, efectiva y ordenada a la información
incidentes de seguridad.
A.16.1.2
Información de informes
eventos de seguridad
Controlar
Los eventos de seguridad de la información se informarán a través de

canales de gestión lo más rápido posible.
A.16.1.3
Información de informes
debilidades de seguridad
Controlar
Empleados y contratistas que utilizan la información de la organización.
Se requerirá que los sistemas y servicios anoten e informen
debilidades de seguridad de la información observadas o sospechadas en el sistema
Tems o servicios.
A.16.1.4
Evaluación de y
decisión sobre información
eventos de seguridad
Controlar
Se evaluarán los eventos de seguridad de la información y se
decidió si deben clasificarse como incidentes de seguridad de la información
abolladuras
A.16.1.5
Respuesta a la información
Control de incidentes de seguridad
Los incidentes de seguridad de la información se responderán de acuerdo con
con los procedimientos documentados
A.16.1.6
Aprendiendo de
seguridad de información
incidentes
Controlar
Conocimiento adquirido al analizar y resolver la seguridad de la información
Los incidentes urbanos se utilizarán para reducir la probabilidad o el impacto de
futuros incidentes
A.16.1.7 Colección de evidencia *Control*
La organización debe definir y aplicar procedimientos para la iden-
tificación, recopilación, adquisición y preservación de información,
que puede servir como evidencia.
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.
A.17.1 Continuidad de seguridad de la información
Objetivo: La continuidad de la seguridad de la información se integrará en la continuidad del negocio de la organización.
sistemas de gestión de ity.
A.17.1.1
Información de planificación
continuidad de seguridad
Controlar
La organización debe determinar sus requisitos de información.
seguridad 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
Implementando información
continuación de seguridad
nuity
Controlar
La organización debe establecer, documentar, implementar y mantener
contener procesos, procedimientos y controles para garantizar lo requerido
nivel de continuidad para la seguridad de la información durante una situación adversa
ción
Tabla A.1 *(continuación)*

A.17.1.3
Verificar, revisar y
evaluar información
continuidad de seguridad
Controlar
La organización debe verificar lo establecido e implementado
controles de continuidad de seguridad de la información a intervalos regulares en
para garantizar que sean válidos y efectivos durante situaciones adversas
situaciones

A.17.2 Despidos

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

A.17.2.1
Disponibilidad de información
procesamiento de mation
instalaciones
Controlar
Las instalaciones de procesamiento de información se implementarán con redun-
Dancy suficiente para cumplir con los requisitos de disponibilidad.

A.18 Cumplimiento

A.18.1 Cumplimiento de los requisitos legales y contractuales.

Objetivo: evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la información
seguridad de mation y de cualquier requisito de seguridad.

A.18.1.1
Identificación de aplicaciones
legislación por cable y
requerimiento contractual
ments
Controlar
Todos los requisitos legislativos, reglamentarios, contractuales relevantes
ments y el enfoque de la organización para cumplir con estos requisitos
deberá ser explícitamente identificado, documentado y actualizado para
cada sistema de información y la organización.

A.18.1.2
Propiedad intelectual
derechos
Controlar
Se implementarán procedimientos apropiados para asegurar el cumplimiento
cumplimiento de los requisitos legislativos, reglamentarios y contractuales
relacionado con los derechos de propiedad intelectual y el uso de software propietario
productos de consumo.

A.18.1.3 Protección de registros *Control*
Los registros estarán protegidos contra pérdida, destrucción, falsificación,
acceso no autorizado y liberación no autorizada, de acuerdo con
requisitos legislativos, reglamentarios, contractuales y comerciales.

A.18.1.4
Privacidad y proteccion
de identificación personal
información capaz
Controlar
La privacidad y protección de la información de identificación personal deberá
Asegurarse como se requiere en la legislación y regulación pertinente donde
aplicable.

A.18.1.5
Regulación de la criptografía
controles gráficos
Controlar
Los controles criptográficos se utilizarán de conformidad con todos los rel
Acuerdos, legislación y normativa vigentes.

A.18.2 Revisiones de seguridad de la información

Objetivo: garantizar que la seguridad de la información se implemente y opere de acuerdo con
Políticas y procedimientos organizacionales.

A.18.2.1
Revisión independiente de
seguridad de información
Controlar
El enfoque de la organización para gestionar la seguridad de la información y
su implementación (es decir, objetivos de control, controles, políticas, pro
se revisarán los procesos y procedimientos de seguridad de la información)
independientemente a intervalos planificados o cuando haya cambios significativos
ocurrir.

Tabla A.1 *(continuación)*

A.18.2.2
Conforme con
políticas de seguridad y
normas
Controlar
Los gerentes deberán revisar periódicamente el cumplimiento de la información.
procesamiento y procedimientos dentro de su área de responsabilidad con
Las políticas de seguridad apropiadas, estándares y cualquier otra seguridad
requisitos

A.18.2.3
Conformidad técnica
revisión
Controlar
Los sistemas de información se revisarán periódicamente para verificar su cumplimiento.
con las políticas y el soporte de seguridad de la información de la organización
ards

Tabla A.1 *(continuación)*

Bibliografía

[1]
ISO / CEI 27002: 2013, *Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información*

[2]
ISO / CEI 27003, *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información*

guía de implementación del sistema
[3]
ISO / CEI 27004, *Tecnología de la información - Técnicas de seguridad - Seguridad de la información gestión - Medición*
[4]
ISO / CEI 27005, *Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información*
[5]
ISO 31000: 2009, *Gestión de riesgos - Principios y directrices*
[6]
Directivas ISO / IEC, Parte 1, *Suplemento ISO consolidado - Procedimientos específicos de ISO* , 2012

ICS 35.040
Precio basado en 23 páginas