INTERNACIONAL ESTÁNDAR

ISO / CEI 27002

Tercera edicion
2022-02

Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información

Seguridad de la información, ciberseguridad y protección de la vida privada - Medidas de seguridad de la información

Número de referencia
ISO/IEC 27002: 2022 (E)

oficina de derechos de autor ISO
CP 401 • Cap. de Blandonnet 8
CH-1214 Vernier, Ginebra
Teléfono: +41 22 749 01 11 Correo
electrónico: copyright@iso.org
Sitio web: www.iso.org

Publicado en Suiza

Contenido

Página

Prefacio

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO e IEC, también participan en el trabajo.

Los procedimientos utilizados para desarrollar este documento y los previstos para su posterior mantenimiento se describen en las Directivas ISO / IEC, Parte 1. En particular, se deben tener en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento fue redactado de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (verwww.iso.org/directivas o www.iec.ch/members_experts/refdocs).

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. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (verwww.iso.org/patents) o la lista IEC de declaraciones de patentes recibidas (verpatentes.iec.ch).

Cualquier nombre comercial utilizado en este documento es información proporcionada para la comodidad de los usuarios y no constituye un respaldo.

Para obtener una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los obstáculos técnicos al comercio (TBT), consulte www.iso.org/iso/prefacio.html . En la CEI, véasewww.iec.ch/understanding-standards .

'Este documento fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1,*Tecnologías de la información*, Subcomité SC 27,*Seguridad de la información, ciberseguridad y protección de la privacidad*.

Esta tercera edición anula y reemplaza a la segunda edición (ISO/IEC 27002:2013), que ha sido revisada técnicamente. También incorpora la Corrección Técnica ISO/IEC 27002:2013/Cor. 1:2014 e ISO/IEC 27002:2013/Cor. 2: 2015.

Los principales cambios son los siguientes:

- el título ha sido modificado;

- se ha cambiado la estructura del documento, presentando los controles utilizando una taxonomía simple y atributos asociados;

- se fusionaron algunos controles, se eliminaron algunos y se introdujeron varios controles nuevos. La correspondencia completa se encuentra enAnexo B .

Cualquier comentario o pregunta sobre este documento debe dirigirse al organismo nacional de normalización del usuario. Una lista completa de estos organismos se puede encontrar enwww.iso.org/members.html y www.iec.ch/comités-nacionales .

Introducción

0.1 Antecedentes y contexto

Este documento está diseñado para organizaciones de todos los tipos y tamaños. Debe usarse como referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001. También puede usarse como documento de orientación para organizaciones que determinan e implementan controles de seguridad de la información. Además, este documento está diseñado para usarse en el desarrollo de pautas de gestión de seguridad de la información específicas de la industria y la organización, teniendo en cuenta su (s) entorno (s) de riesgo de seguridad de la información específico (s). Los controles específicos de la organización o del entorno que no sean los incluidos en este documento se pueden determinar a través de la evaluación de riesgos, según sea necesario.

Las organizaciones de todos los tipos y tamaños (incluidos los sectores público y privado, comerciales y sin fines de lucro) crean, recopilan, procesan, almacenan, transmiten y eliminan información en muchas formas, incluidas las electrónicas, físicas y verbales (por ejemplo, conversaciones y presentaciones).

El valor de la información va más allá de las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y otros activos asociados merecen o requieren protección contra diversas fuentes de riesgo, ya sean naturales, accidentales o deliberadas.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas políticas, reglas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Para cumplir con sus objetivos comerciales y de seguridad específicos, la organización debe definir, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario. Un SGSI como el especificado en ISO/IEC 27001 adopta una visión holística y coordinada de los riesgos de seguridad de la información de la organización para determinar e implementar un conjunto integral de controles de seguridad de la información dentro del marco general de un sistema de gestión coherente.

Muchos sistemas de información, incluidas su gestión y operaciones, no han sido diseñados para ser seguros en términos de un SGSI, como se especifica en ISO/IEC 27001 y este documento. El nivel de seguridad que solo se puede lograr a través de medidas tecnológicas es limitado y debe estar respaldado por actividades de gestión y procesos organizacionales apropiados. Identificar qué controles deben implementarse requiere una planificación cuidadosa y atención a los detalles al llevar a cabo el tratamiento de riesgos.

Un SGSI exitoso requiere el apoyo de todo el personal de la organización. También puede requerir la participación de otras partes interesadas, como accionistas o proveedores. También puede ser necesario el asesoramiento de expertos en la materia.

Un sistema de gestión de la seguridad de la información adecuado, adecuado y eficaz proporciona garantías a la dirección de la organización y a otras partes interesadas de que su información y otros activos asociados se mantienen razonablemente seguros y protegidos contra amenazas y daños, lo que permite a la organización alcanzar los objetivos comerciales establecidos.

0.2 Requisitos de seguridad de la información

Es esencial que una organización determine sus requisitos de seguridad de la información. Hay tres fuentes principales de requisitos de seguridad de la información:

a) la evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos comerciales generales de la organización. Esto se puede facilitar o respaldar a través de una evaluación de riesgos específica de la seguridad de la información. Esto debería resultar en la determinación de los controles necesarios para asegurar que el riesgo residual para la organización cumpla con sus criterios de aceptación del riesgo;

b) los requisitos legales, estatutarios, reglamentarios y contractuales que debe cumplir una organización y sus partes interesadas (socios comerciales, proveedores de servicios, etc.) y su entorno sociocultural;

c) el conjunto de principios, objetivos y requisitos comerciales para todos los pasos del ciclo de vida de la información que una organización ha desarrollado para respaldar sus operaciones.

0.3 Controles

Un control se define como una medida que modifica o mantiene el riesgo. Algunos de los controles en este documento son controles que modifican el riesgo, mientras que otros mantienen el riesgo. Una política de seguridad de la información, por ejemplo, solo puede mantener el riesgo, mientras que el cumplimiento de la política de seguridad de la información puede modificar el riesgo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Este documento proporciona una combinación genérica de controles de seguridad de la información organizacionales, de personas, físicos y tecnológicos derivados de las mejores prácticas reconocidas internacionalmente.

0.4 Determinación de controles

La determinación de los controles depende de las decisiones de la organización luego de una evaluación de riesgos, con un alcance claramente definido. Las decisiones relacionadas con los riesgos identificados deben basarse en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque de gestión del riesgo aplicado por la organización. La determinación de los controles también debe tener en cuenta todas las leyes y reglamentos nacionales e internacionales pertinentes. La determinación del control también depende de la forma en que los controles interactúan entre sí para brindar una defensa en profundidad.

La organización puede diseñar controles según sea necesario o identificarlos de cualquier fuente. Al especificar dichos controles, la organización debe considerar los recursos y la inversión necesarios para implementar y operar un control contra el valor comercial realizado. Consulte ISO / IEC TR 27016 para obtener orientación sobre las decisiones relacionadas con la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de los requisitos competitivos de recursos.

Debe haber un equilibrio entre los recursos desplegados para implementar los controles y el posible impacto comercial resultante de los incidentes de seguridad en ausencia de esos controles. Los resultados de una evaluación de riesgos deben ayudar a guiar y determinar la acción de gestión adecuada, las prioridades para gestionar los riesgos de seguridad de la información y para implementar los controles que se determinen necesarios para proteger contra estos riesgos.

Algunos de los controles de este documento pueden considerarse como principios rectores para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Se puede encontrar más información sobre la determinación de controles y otras opciones de tratamiento de riesgos en ISO / IEC 27005.

0.5 Elaboración de directrices específicas para la organización

Este documento puede considerarse como un punto de partida para el desarrollo de directrices específicas de la organización. No todos los controles y la orientación de este documento pueden aplicarse a todas las organizaciones. También pueden ser necesarios controles y directrices adicionales no incluidos en este documento para abordar las necesidades específicas de la organización y los riesgos que se han identificado. Cuando se desarrollan documentos que contienen pautas o controles adicionales, puede ser útil incluir referencias cruzadas a las cláusulas de este documento para referencia futura.

0.6 Consideraciones sobre el ciclo de vida

La información tiene un ciclo de vida, desde su creación hasta su eliminación. El valor y los riesgos de la información pueden variar a lo largo de este ciclo de vida (p. ej., la divulgación no autorizada o el robo de las cuentas financieras de una empresa no son significativos una vez que se han publicado, pero la integridad sigue siendo crítica); por lo tanto, la seguridad de la información sigue siendo importante hasta cierto punto en todas las etapas

Los sistemas de información y otros activos relevantes para la seguridad de la información tienen ciclos de vida dentro de los cuales se conciben, especifican, diseñan, desarrollan, prueban, implementan, usan, mantienen y finalmente se retiran del servicio y se desechan. La seguridad de la información debe ser considerada en cada etapa. Los proyectos de desarrollo de nuevos sistemas y los cambios en los sistemas existentes brindan oportunidades para mejorar los controles de seguridad al tiempo que se tienen en cuenta los riesgos de la organización y las lecciones aprendidas de los incidentes.

0.7 Normas internacionales relacionadas

Si bien este documento ofrece orientación sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones diferentes, otros documentos de la familia ISO/IEC 27000 brindan consejos o requisitos complementarios sobre otros aspectos del proceso general de gestión de la seguridad de la información.

Consulte ISO/IEC 27000 para obtener una introducción general tanto al SGSI como a la familia de documentos. ISO/IEC 27000 proporciona un glosario que define la mayoría de los términos utilizados en toda la familia de documentos ISO/IEC 27000 y describe el alcance y los objetivos de cada miembro de la familia.

Existen estándares específicos del sector que tienen controles adicionales que apuntan a abordar áreas específicas (p. ej., ISO/IEC 27017 para servicios en la nube, ISO/IEC 27701 para privacidad, ISO/IEC 27019 para energía, ISO/IEC 27011 para organizaciones de telecomunicaciones e ISO 27799 por salud). Dichos estándares se incluyen en la Bibliografía y algunos de ellos se mencionan en las secciones de orientación y otra información enCláusulas 5 -8 .

Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información

1 Alcance

Este documento proporciona un conjunto de referencia de controles genéricos de seguridad de la información, incluida una guía de implementación. Este documento está diseñado para ser utilizado por organizaciones:

a) dentro del contexto de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001;

b) para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente;

c) para desarrollar directrices de gestión de la seguridad de la información específicas de la organización.

2 Referencias normativas

No hay referencias normativas en este documento.

3 Términos, definiciones y términos abreviados

3.1 Términos y definiciones

A los efectos de este documento, se aplican los siguientes términos y definiciones.

ISO e IEC mantienen bases de datos de terminología para su uso en la normalización en las siguientes direcciones:

- Plataforma de navegación ISO Online: disponible enhttps://www.iso.org/obp

- Electropedia IEC: disponible enhttps://www.electropedia.org/

3.1.1
control de acceso
medios para asegurar que el acceso físico y lógico a*activos*(3.1.2) está autorizado y restringido en función de los requisitos comerciales y de seguridad de la información

3.1.2
activo
cualquier cosa que tenga valor para la organización

Nota 1 a la entrada: En el contexto de la seguridad de la información, se pueden distinguir dos tipos de activos:

- los activos primarios:

  - información;

  - negocio*procesos*(3.1.27) y actividades;

- los activos de apoyo (de los que dependen los activos primarios) de todo tipo, por ejemplo:

  - ferretería;

  - software;

  - la red;

  - *personal*(3.1.20);

- sitio;

- la estructura de la organización.

3.1.3
ataque
intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un *activo* (3.1.2) o cualquier intento de exponer, robar o hacer uso no autorizado de un *activo* (3.1.2)

3.1.4
autenticación
garantía de que una característica reivindicada de un *entidad* (3.1.11) es correcto

3.1.5
autenticidad
propiedad que un *entidad* (3.1.11) es lo que dice ser

3.1.6
cadena de custodia
posesión demostrable, movimiento, manejo y ubicación de material de un punto en el tiempo a otro

Nota 1 a la entrada: El material incluye información y otros datos asociados. *activos* (3.1.2) en el contexto de ISO/IEC 27002.

[FUENTE: ISO/IEC 27050-1: 2019, 3.1, modificado - “Nota 1 a la entrada” añadida]

3.1.7
información confidencial
información que no está destinada a estar disponible o divulgada a personas no autorizadas, *entidades* (3.1.11) o *procesos* (3.1.27)

3.1.8
control
medida que mantiene y/o modifica el riesgo

Nota 1 a la entrada: Los controles incluyen, entre otros, cualquier *proceso* (3.1.27), *política* (3.1.24), dispositivo, práctica u otras condiciones y/o acciones que mantienen y/o modifican el riesgo.

Nota 2 a la entrada: Es posible que los controles no siempre ejerzan el efecto de modificación pretendido o asumido.

[FUENTE: ISO 31000: 2018, 3.8]

3.1.9
ruptura
incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización

[FUENTE: ISO 22301: 2019, 3.10]

3.1.10
dispositivo de punto final
dispositivo de hardware de tecnología de la información y la comunicación (TIC) conectado a la red

Nota 1 a la entrada: Dispositivo de punto final puede referirse a computadoras de escritorio, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, impresoras u otro hardware especializado, incluidos medidores inteligentes y dispositivos de Internet de las cosas (IoT).

3.1.11
entidad
elemento relevante para el propósito de la operación de un dominio que tiene una existencia reconociblemente distinta

Nota 1 a la entrada: Una entidad puede tener una realización física o lógica.

EJEMPLO Una persona, una organización, un dispositivo, un grupo de tales elementos, un suscriptor humano de una empresa de telecomunicaciones. servicio, una tarjeta SIM, un pasaporte, una tarjeta de interfaz de red, una aplicación de software, un servicio o un sitio web.

[FUENTE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12

instalación de procesamiento de información

cualquier sistema, servicio o infraestructura de procesamiento de información, o la ubicación física que lo alberga

[FUENTE: ISO/IEC 27000: 2018, 3.27, modificado - "facilities" ha sido reemplazado por facilidad.]

3.1.13

violación de la seguridad de la información

compromiso de la seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a la información protegida transmitida, almacenada o procesada de otro modo

3.1.14

evento de seguridad de la información

ocurrencia que indica una posible *violación de la seguridad de la información* (3.1.13) o fallo de *control S* (3.1.8)

[FUENTE: ISO/IEC 27035-1: 2016, 3.3, modificada - “violación de la seguridad de la información” ha sido reemplazada por “violación de la seguridad de la información”]

3.1.15

incidente de seguridad de la información

uno o varios relacionados e identificados *eventos de seguridad de la información* (3.1.14) que pueden dañar la organización *activos* (3.1.2) o comprometer sus operaciones

[FUENTE: ISO/IEC 27035-1: 2016, 3.4]

3.1.16

gestión de incidentes de seguridad de la información

ejercicio de un enfoque consistente y efectivo para el manejo de *incidentes de seguridad de la información* (3.1.15)

[FUENTE: ISO/IEC 27035-1: 2016, 3.5]

3.1.17

sistema de informacion

conjunto de aplicaciones, servicios, tecnología de la información *activos* (3.1.2), u otros componentes de manejo de información

[FUENTE: ISO/IEC 27000:2018, 3.35]

3.1.18

parte interesada

Interesado

persona u organización que puede afectar, ser afectada o percibirse a sí misma como afectada por una decisión o actividad

[FUENTE: ISO/IEC 27000:2018, 3.37]

3.1.19

no repudio

capacidad de probar la ocurrencia de un evento o acción reclamada y su origen *entidades* (3.1.11)

3.1.20

personal

personas que trabajan bajo la dirección de la organización

Nota 1 a la entrada: El concepto de personal incluye a los miembros de la organización, tales como el órgano de gobierno, la alta dirección, los empleados, el personal temporal, los contratistas y los voluntarios.

3.1.21
información de identificación personal
PII
cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o (b) esté o pueda estar vinculada directa o indirectamente a una persona física.

Nota 1 a la entrada: La "persona física" en la definición es la *director de información personal identificable* (3.1.22). Para determinar si un principal de PII es identificable, se deben tener en cuenta todos los medios que razonablemente puede utilizar la parte interesada en la privacidad que posee los datos, o cualquier otra parte, para establecer el vínculo entre el conjunto de PII y la persona física.

[FUENTE: ISO / IEC 29100: 2011 / Amd.1: 2018, 2.9]

3.1.22
director de información personal identificable
persona natural a quien el *información de identificación personal (PII)* (3.1.21) se relaciona

Nota 1 a la entrada: Dependiendo de la jurisdicción y de la legislación particular de privacidad y protección de datos, también se puede usar el sinónimo "sujeto de datos" en lugar del término "principal de PII".

[FUENTE: ISO/IEC 29100: 2011, 2.11]

3.1.23
procesador de información personal
parte interesada en privacidad que procesa *información de identificación personal (PII)* (3.1.21) en nombre y de acuerdo con las instrucciones de un controlador de PII

[FUENTE: ISO/IEC 29100: 2011, 2.12]

3.1.24
política
Intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

[FUENTE: ISO/IEC 27000: 2018, 3.53]

3.1.25
evaluación de impacto en la privacidad
PIA
en general *proceso* (3.1.27) de identificar, analizar, evaluar, consultar, comunicar y planificar el tratamiento de los posibles impactos sobre la privacidad en relación con el tratamiento de *información de identificación personal (PII)* (3.1.21), enmarcado dentro del marco más amplio de gestión de riesgos de una organización

[FUENTE: ISO/IEC 29134: 2017, 3.7, modificado - Nota 1 a la entrada eliminada.]

3.1.26
procedimiento
forma específica de llevar a cabo una actividad o una *proceso* (3.1.27)

[FUENTE: ISO 30000: 2009, 3.12]

3.1.27
proceso
conjunto de actividades interrelacionadas o que interactúan que usa o transforma entradas para entregar un resultado

[FUENTE: ISO 9000: 2015, 3.4.1, modificada— Notas a la entrada eliminadas.]

3.1.28
registro
información creada, recibida y mantenida como evidencia y como *activo* (3.1.2) por una organización o persona, en cumplimiento de obligaciones legales o en la transacción de negocios

Nota 1 a la entrada: Las obligaciones legales en este contexto incluyen todos los requisitos legales, estatutarios, reglamentarios y contractuales.

[ORIGEN: ISO 15489-1: 2016, 3.14, modificado—"Nota 1 a la entrada" agregada.]

3.1.29
punto de recuperación objetivo
RPO
punto en el tiempo en el que se van a recuperar los datos después de un*ruptura*(3.1.9) ha ocurrido

[FUENTE: ISO / IEC 27031: 2011, 3.12, modificado - "debe" reemplazado por "debe ser".]

3.1.30
tiempo de recuperación objetivo
RTO
período de tiempo dentro del cual se recuperarán los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte después de una*ruptura*(3.1.9) ha ocurrido

[FUENTE: ISO / IEC 27031: 2011, 3.13, modificado - "debe" reemplazado por "debe ser".]

3.1.31
fiabilidad
propiedad de comportamiento y resultados consistentes previstos

3.1.32
regla
principio aceptado o instrucción que establece las expectativas de la organización sobre lo que se requiere hacer, lo que está permitido o no permitido

Nota 1 a la entrada: Las reglas pueden expresarse formalmente en*políticas de temas específicos*(3.1.35) y en otro tipo de documentos.

3.1.33
información sensible
información que debe protegerse de la falta de disponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en un individuo, organización, seguridad nacional o seguridad pública

3.1.34
amenaza
causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización

[FUENTE: ISO/IEC 27000:2018, 3.74]

3.1.35
política específica del tema
Intenciones y dirección sobre un tema o tema específico, según lo expresado formalmente por el nivel apropiado de gestión.

Nota 1 a la entrada: Las políticas específicas de un tema pueden expresar formalmente*normas*(3.1.32) o normas de la organización.

Nota 2 a la entrada: Algunas organizaciones usan otros términos para estas políticas de temas específicos.

Nota 3 a la entrada: Las políticas específicas del tema a las que se hace referencia en este documento están relacionadas con la seguridad de la información.

EJEMPLO Política específica de un tema sobre*control de acceso*(3.1.1), política específica del tema sobre escritorio despejado y pantalla despejada.

3.1.36
usuario
parte interesada(3.1.18) con acceso a la organización*sistemas de información*(3.1.17)

EJEMPLO *Personal*(3.1.20), clientes, proveedores.

3.1.37

dispositivo de punto final del usuario

dispositivo de punto final (3.1.10) utilizados por los usuarios para acceder a los servicios de procesamiento de información

Nota 1 a la entrada: El dispositivo de punto final del usuario puede referirse a computadoras de escritorio, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, etc.

3.1.38

vulnerabilidad

debilidad de un *activo* (3.1.2) o *control* (3.1.8) que pueden ser explotados por uno o más *amenazas* (3.1.34)

[FUENTE: ISO/IEC 27000:2018, 3.77]

3.2 Términos abreviados

ABAC	control de acceso basado en atributos
LCA	lista de control de acceso
BIA	Análisis de Impacto del Negocio
BYOD	trae tu propio dispositivo

CAPTCHA Prueba de Turing pública totalmente automatizada para diferenciar a las computadoras de los humanos

UPC	unidad Central de procesamiento
CAD	control de acceso discrecional
DNS	sistema de nombres de dominio
GPS	sistema de Posicionamiento Global
SOY	gestión de identidad y acceso
TIC	tecnología de la información y la comunicación
IDENTIFICACIÓN	identificar
IDE	entorno de desarrollo integrado
DNI	sistema de detección de intrusos
internet de las cosas	Internet de las Cosas
IP	protocolo de Internet
IPS	Sistema de Prevención de Intrusión
ESO	tecnologías de la información
SGSI	sistema de gestión de seguridad de la información
MAC	control de acceso obligatorio
NTP	Protocolo de tiempo de red
PIA	evaluación del impacto en la privacidad
información personal	información de identificación personal

ALFILER	número de identificación personal
PKI	Infraestructura de Clave Pública
PTP	protocolo de tiempo de precisión
RBAC	control de acceso basado en roles
RPO	objetivo de punto de recuperación
RTO	objetivo de tiempo de recuperación
SAST	pruebas de seguridad de aplicaciones estáticas
Dakota del Sur	Seguro digital
SDN	Redes definidas por software
SD-WAN	redes de área amplia definidas por software
SIEM	información de seguridad y gestión de eventos
SMS	servicio de mensajes cortos
sql	lenguaje de consulta estructurado
inicio de sesión único	inicio de sesión único
SWID	identificación de software
UEBA	análisis de comportamiento de usuarios y entidades
UPS	fuente de poder ininterrumpible
URL	Localizador Uniforme de Recursos
USB	bus serie universal
máquina virtual	máquina virtual
vpn	red privada virtual
Wifi	fidelidad inalámbrica

4 Estructura de este documento

4.1 Cláusulas

Este documento está estructurado de la siguiente manera:

a) Controles organizacionales (Cláusula 5)

b) Controles de personas (Cláusula 6)

c) Controles físicos (Cláusula 7)

d) Controles tecnológicos (Cláusula 8)

Hay 2 anexos informativos:

- Anexo A - Uso de atributos

- Anexo B - Correspondencia con ISO/IEC 27002:2013

Anexo A explica cómo una organización puede usar atributos (ver4.2) para crear sus propias vistas basadas en los atributos de control definidos en este documento o de creación propia.

Anexo B muestra la correspondencia entre los controles en esta edición de ISO/IEC 27002 y la edición anterior de 2013.

4.2 Temas y atributos

La categorización de los controles dada enCláusulas 5 para8 se denominan temas.

Los controles se clasifican como:

a) personas, si se refieren a personas individuales;

b) físicos, si se trata de objetos físicos;

c) tecnológicos, si se trata de tecnología;

d) en caso contrario se categorizan como organizacionales.

La organización puede usar atributos para crear diferentes vistas que son diferentes categorizaciones de controles vistos desde una perspectiva diferente a los temas. Los atributos se pueden usar para filtrar, ordenar o presentar controles en diferentes vistas para diferentes audiencias.Anexo A explica cómo se puede lograr esto y proporciona un ejemplo de una vista.

A modo de ejemplo, cada control en este documento se ha asociado con cinco atributos con los valores de atributos correspondientes (precedidos por "#" para que se puedan buscar), de la siguiente manera:

a) Tipo de control

> El tipo de control es un atributo para ver los controles desde la perspectiva de cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información. Los valores de los atributos consisten en Preventivo (el control que tiene como objetivo prevenir la ocurrencia de un incidente de seguridad de la información), Detectivo (el control actúa cuando ocurre un incidente de seguridad de la información) y Correctivo (el control actúa después de que ocurre un incidente de seguridad de la información).

b) Propiedades de seguridad de la información

> Las propiedades de seguridad de la información son un atributo para ver los controles desde la perspectiva de qué característica de la información el control contribuirá a preservar. Los valores de los atributos consisten en Confidencialidad, Integridad y Disponibilidad.

c) Conceptos de ciberseguridad

> Conceptos de ciberseguridad es un atributo para ver los controles desde la perspectiva de la asociación de controles a los conceptos de ciberseguridad definidos en el marco de trabajo de ciberseguridad descrito en ISO/IEC TS 27110. Los valores de atributo consisten en Identificar, Proteger, Detectar, Responder y Recuperar.

d) Capacidades operativas

> Las capacidades operativas son un atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Los valores de los atributos consisten en Gobernanza, Gestión_de_activos, Protección_de_la_información, Seguridad_de_recursos_humanos, Seguridad_física, Seguridad_de_sistemas_y_redes, Seguridad_de_aplicaciones, Configuración_segura, Gestión_de_identidades_y_accesos, Gestión_de_amenazas_y_vulnerabilidades, Continuidad, Relaciones_con_proveedores_y_seguridad_y_seguridad_de_las_relaciones_de_la_información.

e) Dominios de seguridad

Los dominios de seguridad son un atributo para ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: "Gobierno y ecosistema" incluye "Gobierno de seguridad del sistema de información y gestión de riesgos" y "Gestión de ciberseguridad del ecosistema" (incluidas las partes interesadas internas y externas); "Protección" incluye "Arquitectura de seguridad de TI", "Administración de seguridad de TI", "Gestión de acceso e identidad", "Mantenimiento de seguridad de TI" y "Seguridad física y ambiental"; “Defensa” incluye “Detección” y “Gestión de Incidentes de Seguridad Informática”; “Resiliencia” incluye “Continuidad de operaciones” y “Gestión de crisis”. Los valores de atributo consisten en Gobernanza_y_Ecosistema, Protección, Defensa y Resiliencia.

Los atributos proporcionados en este documento se seleccionan porque se consideran lo suficientemente genéricos para ser utilizados por diferentes tipos de organizaciones. Las organizaciones pueden optar por ignorar uno o más de los atributos proporcionados en este documento. También pueden crear sus propios atributos (con los valores de atributos correspondientes) para crear sus propias vistas organizativas.Cláusula A.2 incluye ejemplos de tales atributos.

4.3 Diseño de controles

El diseño de cada control contiene lo siguiente:

- **Título de control:**Nombre corto del control;
- **Tabla de atributos**: Una tabla muestra el valor (s) de cada atributo para el control dado;
- **Control:**Cuál es el control;
- **Propósito**: Por qué se debe implementar el control;
- **Guia:**Cómo se debe implementar el control;
- **Otra información:**Texto explicativo o referencias a otros documentos relacionados.

Los subtítulos se utilizan en el texto de guía para algunos controles para facilitar la lectura cuando la guía es larga y aborda varios temas. Dichos encabezados no se utilizan necesariamente en todos los textos de orientación. Los subtítulos sonsubrayada .

5 Controles organizacionales

5.1 Políticas de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_y_Eco-sistema #Resiliencia

Control

La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.

Propósito

Garantizar la idoneidad, la adecuación y la eficacia continuas de la dirección de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos comerciales, legales, estatutarios, reglamentarios y contractuales.

Guia

Al más alto nivel, la organización debería definir una “política de seguridad de la información” que sea aprobada por la alta dirección y que establezca el enfoque de la organización para gestionar su seguridad de la información.

La política de seguridad de la información debe tomar en consideración los requisitos derivados de:

a) estrategia comercial y requisitos;

b) reglamentos, legislación y contratos;

c) los riesgos y amenazas actuales y proyectados para la seguridad de la información.

La política de seguridad de la información debe contener declaraciones relativas a:

a) definición de seguridad de la información;

b) los objetivos de seguridad de la información o el marco para establecer los objetivos de seguridad de la información;

c) principios para guiar todas las actividades relacionadas con la seguridad de la información;

d) compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información;

e) compromiso con la mejora continua del sistema de gestión de seguridad de la información;

f) asignación de responsabilidades para la gestión de la seguridad de la información a roles definidos;

(g) procedimientos para el manejo de exenciones y excepciones.

La alta dirección debe aprobar cualquier cambio en la política de seguridad de la información.

En un nivel inferior, la política de seguridad de la información debe estar respaldada por políticas específicas del tema según sea necesario, para exigir aún más la implementación de controles de seguridad de la información. Las políticas de temas específicos generalmente se estructuran para abordar las necesidades de ciertos grupos objetivo dentro de una organización o para cubrir ciertas áreas de seguridad. Las políticas específicas de un tema deben estar alineadas y complementarse con la política de seguridad de la información de la organización.

Ejemplos de tales temas incluyen:

a) control de acceso;

b) seguridad física y ambiental;

c) gestión de activos;

d) transferencia de información;

e) configuración y manejo seguros de los dispositivos de punto final del usuario;

f) seguridad de redes;

g) gestión de incidentes de seguridad de la información;

h) copia de seguridad;

i) criptografía y gestión de claves;

j) clasificación y manejo de la información;

k) gestión de vulnerabilidades técnicas;

l) desarrollo seguro.

La responsabilidad del desarrollo, revisión y aprobación de las políticas específicas del tema debe asignarse al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica. La revisión debe incluir la evaluación de las oportunidades de mejora de la política de seguridad de la información de la organización y las políticas específicas del tema y la gestión de la seguridad de la información en respuesta a los cambios en:

a) la estrategia comercial de la organización;

b) el entorno técnico de la organización;

c) reglamentos, estatutos, legislación y contratos;

d) riesgos de seguridad de la información;

e) el entorno actual y proyectado de amenazas a la seguridad de la información;

f) lecciones aprendidas de eventos e incidentes de seguridad de la información.

La revisión de la política de seguridad de la información y las políticas específicas del tema deben tener en cuenta los resultados de las revisiones y auditorías de gestión. Se debe considerar la revisión y actualización de otras políticas relacionadas cuando se cambia una política para mantener la coherencia.

La política de seguridad de la información y las políticas específicas del tema deben comunicarse al personal relevante y a las partes interesadas en una forma que sea relevante, accesible y comprensible para el lector previsto. Se debe exigir a los destinatarios de las políticas que reconozcan que comprenden y aceptan cumplir con las políticas cuando corresponda. La organización puede determinar los formatos y nombres de estos documentos de política que satisfagan las necesidades de la organización. En algunas organizaciones, la política de seguridad de la información y las políticas específicas del tema pueden estar en un solo documento. La organización puede denominar a estas políticas temáticas como estándares, directivas, políticas u otros.

Si la política de seguridad de la información o cualquier política específica de un tema se distribuye fuera de la organización, se debe tener cuidado de no revelar información confidencial de manera inapropiada.

tabla 1 ilustra las diferencias entre la política de seguridad de la información y la política específica de un tema.

Tabla 1: Diferencias entre la política de seguridad de la información y la política específica del tema

	política de seguridad de la información	Política de temas específicos
Nivel de detalle	General o de alto nivel	Específico y detallado
Documentado y aprobado formalmente por	alta dirección	Nivel adecuado de gestión

Otra información

Las políticas específicas de un tema pueden variar entre organizaciones.

5.2 Roles y responsabilidades de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_y_Ecosistema #Protección #Resiliencia

Control

Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.

Propósito

Establecer una estructura definida, aprobada y entendida para la implementación, operación y gestión de la seguridad de la información dentro de la organización.

Guia

La asignación de funciones y responsabilidades de seguridad de la información debe realizarse de acuerdo con la política de seguridad de la información y las políticas específicas del tema (ver5.1). La organización debería definir y gestionar las responsabilidades para:

a) protección de la información y otros activos asociados;

b) realizar procesos específicos de seguridad de la información;

c) actividades de gestión de riesgos de seguridad de la información y, en particular, aceptación de riesgos residuales (por ejemplo, para los propietarios de riesgos);

d) todo el personal que utiliza la información de una organización y otros activos asociados.

Estas responsabilidades deben complementarse, cuando sea necesario, con una guía más detallada para sitios específicos e instalaciones de procesamiento de información. Las personas con responsabilidades de seguridad de la información asignadas pueden asignar tareas de seguridad a otros. Sin embargo, siguen siendo responsables y deben determinar que las tareas delegadas se hayan realizado correctamente.

Cada área de seguridad de la cual los individuos son responsables debe definirse, documentarse y comunicarse. Los niveles de autorización deben definirse y documentarse. Las personas que asumen una función específica de seguridad de la información deben ser competentes en el conocimiento y las habilidades requeridas por la función y deben recibir apoyo para mantenerse al día con los desarrollos relacionados con la función y necesarios para cumplir con las responsabilidades de la función.

Otra información

Muchas organizaciones designan a un gerente de seguridad de la información para que asuma la responsabilidad general del desarrollo y la implementación de la seguridad de la información y para respaldar la identificación de riesgos y los controles de mitigación.

Sin embargo, la responsabilidad de dotar de recursos e implementar los controles a menudo recae en los gerentes individuales. Una práctica común es designar un propietario para cada activo, quien luego se hace responsable de su protección diaria.

Según el tamaño y los recursos de una organización, la seguridad de la información puede estar cubierta por funciones o funciones dedicadas que se llevan a cabo además de las funciones existentes.

5.3 Segregación de funciones

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gobernanza #identidad_y_ac-cess_management	# Gobernanza_y_Ecosistema

Control

Deben segregarse los deberes conflictivos y las áreas conflictivas de responsabilidad.

Propósito

Reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información.

Guia

La segregación de deberes y áreas de responsabilidad tiene como objetivo separar los deberes en conflicto entre diferentes individuos para evitar que un individuo ejecute deberes potencialmente conflictivos por su cuenta.

La organización debe determinar qué deberes y áreas de responsabilidad deben segregarse. Los siguientes son ejemplos de actividades que pueden requerir segregación:

a) iniciar, aprobar y ejecutar un cambio;

b) solicitar, aprobar e implementar derechos de acceso;

c) diseñar, implementar y revisar el código;

d) desarrollar software y administrar sistemas de producción;

e) usar y administrar aplicaciones;

f) uso de aplicaciones y bases de datos de administración;

g) diseñar, auditar y asegurar los controles de seguridad de la información.

Se debe considerar la posibilidad de colusión al diseñar los controles de segregación. Las organizaciones pequeñas pueden encontrar difícil lograr la segregación de funciones, pero el principio debe aplicarse en la medida de lo posible y practicable. Siempre que sea difícil segregar, se deben considerar otros controles, como el seguimiento de las actividades, las pistas de auditoría y la supervisión de la gestión.

Se debe tener cuidado al utilizar sistemas de control de acceso basados en roles para garantizar que a las personas no se les otorguen roles en conflicto. Cuando hay una gran cantidad de roles, la organización debe considerar el uso de herramientas automatizadas para identificar conflictos y facilitar su eliminación. Los roles deben definirse y aprovisionarse cuidadosamente para minimizar los problemas de acceso si se elimina o reasigna un rol.

Otra información

Ninguna otra información.

5.4 Responsabilidades de la dirección

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_y_Ecosistema

Control

La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.

Propósito

Asegurar que la gerencia comprenda su papel en la seguridad de la información y emprender acciones destinadas a garantizar que todo el personal conozca y cumpla con sus responsabilidades de seguridad de la información.

Guia

La gerencia debe demostrar su apoyo a la política de seguridad de la información, las políticas específicas del tema, los procedimientos y los controles de seguridad de la información.

Las responsabilidades de la gerencia deben incluir asegurar que el personal:

a) estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información antes de que se les conceda acceso a la información de la organización y otros activos asociados;

b) cuentan con lineamientos que establecen las expectativas de seguridad de la información de su rol dentro de la organización;

c) tienen el mandato de cumplir con la política de seguridad de la información y las políticas específicas de la organización;

d) lograr un nivel de conciencia de la seguridad de la información relevante para sus roles y responsabilidades dentro de la organización (ver6.3);

e) el cumplimiento de los términos y condiciones de empleo, contrato o acuerdo, incluida la política de seguridad de la información de la organización y los métodos de trabajo apropiados;

f) continuar teniendo las habilidades y calificaciones apropiadas en seguridad de la información a través de la educación profesional continua;

g) cuando sea factible, cuenten con un canal confidencial para denunciar violaciones de la política de seguridad de la información, políticas específicas de un tema o procedimientos para la seguridad de la información ("denuncia"). Esto puede permitir informes anónimos o tener disposiciones para garantizar que el conocimiento de la identidad del denunciante sea conocido solo por aquellos que deben tratar con dichos informes;

h) cuentan con recursos adecuados y tiempo de planificación de proyectos para implementar los procesos y controles relacionados con la seguridad de la organización.

Otra información

Ninguna otra información.

5.5 Contacto con las autoridades

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger #Responder #Recuperar	# Gobernanza	# Defensa # Resiliencia

Control

La organización debe establecer y mantener contacto con las autoridades pertinentes.

Propósito

Garantizar que se produzca un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reguladoras y de supervisión pertinentes.

Guia

La organización debe especificar cuándo y por quién se debe contactar a las autoridades (p. ej., fuerzas del orden, organismos reguladores, autoridades de supervisión) y cómo se deben informar oportunamente los incidentes de seguridad de la información identificados.

Los contactos con las autoridades también deben utilizarse para facilitar la comprensión de las expectativas actuales y futuras de estas autoridades (por ejemplo, las normas de seguridad de la información aplicables).

Otra información

Las organizaciones bajo ataque pueden solicitar a las autoridades que tomen medidas contra la fuente del ataque.

Mantener dichos contactos puede ser un requisito para respaldar la gestión de incidentes de seguridad de la información (ver5.24 para5.28) o los procesos de planificación de contingencia y continuidad del negocio (ver5.29 y5.30). Los contactos con los organismos reguladores también son útiles para anticipar y prepararse para los próximos cambios en las leyes o reglamentos relevantes que afectan a la organización. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, proveedores de electricidad y salud y seguridad [por ejemplo, departamentos de bomberos (en

conexión con la continuidad del negocio), proveedores de telecomunicaciones (en relación con el enrutamiento y la disponibilidad de la línea) y proveedores de agua (en relación con las instalaciones de refrigeración para equipos)].

5.6 Contacto con grupos de interés especial

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Responder # recuperar	# Gobernanza	# Defensa

Control

La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Propósito

Garantizar que se produzca un flujo adecuado de información con respecto a la seguridad de la información.

Guia

La pertenencia a grupos o foros de intereses especiales debe considerarse como un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante;

b) asegurarse de que la comprensión del entorno de seguridad de la información esté actualizada;

c) recibir alertas tempranas de alertas, avisos y parches relacionados con ataques y vulnerabilidades;

d) obtener acceso a asesoramiento especializado en seguridad de la información;

e) compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades;

f) proporcionar puntos de enlace adecuados cuando se trata de incidentes de seguridad de la información (ver5.24 para5.28).

Otra información

Ninguna otra información.

5.7 Inteligencia de amenazas

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar #Detectar # Responder	# Threat_and_vulner-gestión_de_habilidades	# Defensa # Resiliencia

Control

La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas.

Propósito

Proporcionar conciencia del entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas.

Guia

La información sobre amenazas existentes o emergentes se recopila y analiza para:

a) facilitar acciones informadas para evitar que las amenazas causen daño a la organización;

b) reducir el impacto de tales amenazas.

La inteligencia de amenazas se puede dividir en tres capas, todas las cuales deben tenerse en cuenta:

a) inteligencia de amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques);

b) inteligencia de amenazas tácticas: información sobre las metodologías, herramientas y tecnologías involucradas del atacante;

c) inteligencia de amenazas operativas: detalles sobre ataques específicos, incluidos indicadores técnicos.

La inteligencia de amenazas debe ser:

a) relevante (es decir, relacionado con la protección de la organización);

b) perspicaz (es decir, proporcionar a la organización una comprensión precisa y detallada del panorama de amenazas);

c) contextual, para brindar conciencia situacional (es decir, agregar contexto a la información en función del momento de los eventos, dónde ocurren, experiencias previas y prevalencia en organizaciones similares);

d) procesable (es decir, la organización puede actuar sobre la información de manera rápida y efectiva).

Las actividades de inteligencia de amenazas deben incluir:

a) establecer objetivos para la producción de inteligencia sobre amenazas;

b) identificar, examinar y seleccionar fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información requerida para la producción de inteligencia sobre amenazas;

c) recopilar información de fuentes seleccionadas, que pueden ser internas y externas;

d) procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando la información);

e) analizar la información para comprender cómo se relaciona y es significativa para la organización;

f) comunicarlo y compartirlo con personas relevantes en un formato que pueda ser entendido.

La inteligencia de amenazas debe analizarse y utilizarse posteriormente:

a) implementando procesos para incluir información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización;

b) como entrada adicional a controles técnicos preventivos y de detección como firewalls, sistema de detección de intrusos o soluciones antimalware;

c) como entrada a los procesos y técnicas de prueba de seguridad de la información.

La organización debe compartir la inteligencia sobre amenazas con otras organizaciones de forma mutua para mejorar la inteligencia sobre amenazas en general.

Otra información

Las organizaciones pueden utilizar la inteligencia de amenazas para prevenir, detectar o responder a las amenazas. Las organizaciones pueden producir inteligencia sobre amenazas, pero normalmente reciben y hacen uso de la inteligencia sobre amenazas producida por otras fuentes.

La inteligencia de amenazas a menudo la proporcionan proveedores o asesores independientes, agencias gubernamentales o grupos colaborativos de inteligencia de amenazas.

La efectividad de los controles tales como5.25 ,8.7 ,8.16 o8.23 , depende de la calidad de la inteligencia de amenazas disponible.

5.8 Seguridad de la información en la gestión de proyectos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Gobernanza	# Gobernanza_y_Ecosistema #Protección

Control

La seguridad de la información debe integrarse en la gestión de proyectos.

Propósito

Para garantizar que los riesgos de seguridad de la información relacionados con proyectos y entregables se aborden de manera efectiva en la gestión de proyectos a lo largo del ciclo de vida del proyecto.

Guia

La seguridad de la información debe integrarse en la gestión del proyecto para garantizar que los riesgos de seguridad de la información se aborden como parte de la gestión del proyecto. Esto se puede aplicar a cualquier tipo de proyecto, independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo, un proyecto para un proceso comercial central, TIC, gestión de instalaciones u otros procesos de apoyo).

La gestión de proyectos en uso debe exigir que:

a) los riesgos de seguridad de la información se evalúan y tratan en una etapa temprana y periódicamente como parte de los riesgos del proyecto a lo largo del ciclo de vida del proyecto;

b) requisitos de seguridad de la información [por ejemplo, requisitos de seguridad de la aplicación (8.26), requisitos para cumplir con los derechos de propiedad intelectual (5.32), etc.] se abordan en las primeras etapas de los proyectos;

c) los riesgos de seguridad de la información asociados con la ejecución de proyectos, como la seguridad de los aspectos de comunicación interna y externa, se consideran y tratan a lo largo del ciclo de vida del proyecto;

d) se revisa el progreso en el tratamiento de riesgos de seguridad de la información y se evalúa y prueba la efectividad del tratamiento.

La idoneidad de las consideraciones y actividades de seguridad de la información debe ser objeto de seguimiento en etapas predefinidas por personas u órganos de gobierno adecuados, como el comité directivo del proyecto.

Las responsabilidades y autoridades para la seguridad de la información relevantes para el proyecto deben definirse y asignarse a roles específicos.

Los requisitos de seguridad de la información para los productos o servicios que entregará el proyecto deben determinarse utilizando varios métodos, incluida la derivación de los requisitos de cumplimiento de la política de seguridad de la información, las políticas y las reglamentaciones específicas del tema. Se pueden derivar otros requisitos de seguridad de la información de actividades como el modelado de amenazas, revisiones de incidentes, uso de umbrales de vulnerabilidad o planificación de contingencias, asegurando así que la arquitectura y el diseño de los sistemas de información estén protegidos contra amenazas conocidas basadas en el entorno operativo.

Los requisitos de seguridad de la información deben determinarse para todos los tipos de proyectos, no solo para los proyectos de desarrollo de TIC. También se debe considerar lo siguiente al determinar estos requisitos:

a) qué información está involucrada (determinación de la información), cuáles son las necesidades de seguridad de la información correspondientes (clasificación; véase5.12) y el potencial impacto comercial negativo que puede resultar de la falta de seguridad adecuada;

b) las necesidades de protección requeridas de la información y otros activos asociados involucrados, particularmente en términos de confidencialidad, integridad y disponibilidad;

c) el nivel de confianza o seguridad requerido con respecto a la identidad reclamada de las entidades para derivar los requisitos de autenticación;

d) acceder a los procesos de aprovisionamiento y autorización, para clientes y otros usuarios comerciales potenciales, así como para usuarios privilegiados o técnicos, como miembros relevantes del proyecto, personal de operación potencial o proveedores externos;

e) informar a los usuarios de sus deberes y responsabilidades;

f) requisitos derivados de los procesos comerciales, como el registro y seguimiento de transacciones, requisitos de no repudio;

g) requisitos exigidos por otros controles de seguridad de la información (por ejemplo, interfaces para registro y monitoreo o sistemas de detección de fuga de datos);

h) cumplimiento del entorno legal, estatutario, reglamentario y contractual en el que opera la organización;

i) el nivel de confianza o garantía requerido para que terceros cumplan con la política de seguridad de la información de la organización y las políticas específicas del tema, incluidas las cláusulas de seguridad relevantes en cualquier acuerdo o contrato.

Otra información

El enfoque de desarrollo del proyecto, como el ciclo de vida en cascada o el ciclo de vida ágil, debe respaldar la seguridad de la información de una manera estructurada que pueda adaptarse para adaptarse a la gravedad evaluada de los riesgos de seguridad de la información, según el carácter del proyecto. La consideración temprana de los requisitos de seguridad de la información para el producto o servicio (por ejemplo, en las etapas de planificación y diseño) puede conducir a soluciones más eficaces y rentables para la calidad y la seguridad de la información. ISO 21500 e ISO 21502 brindan orientación sobre conceptos y procesos de gestión de proyectos que son importantes para el desempeño de los proyectos.

ISO/IEC 27005 proporciona orientación sobre el uso de procesos de gestión de riesgos para identificar controles para cumplir con los requisitos de seguridad de la información.

5.9 Inventario de información y otros activos asociados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Asset_manage- mento	# Gobernanza_y_Eco- proteccion del sistema

Control

Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.

Propósito

Identificar la información de la organización y otros activos asociados con el fin de preservar su seguridad de la información y asignar la propiedad adecuada.

Guia

Inventario

La organización debe identificar su información y otros activos asociados y determinar su importancia en términos de seguridad de la información. La documentación debe mantenerse en inventarios dedicados o existentes, según corresponda.

El inventario de información y otros activos asociados debe ser preciso, actualizado, consistente y alineado con otros inventarios. Las opciones para garantizar la precisión de un inventario de información y otros activos asociados incluyen:

a) realizar revisiones periódicas de la información identificada y otros activos asociados contra el inventario de activos;

b) hacer cumplir automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo.

La ubicación de un activo debe incluirse en el inventario según corresponda.

El inventario no necesita ser una lista única de información y otros activos asociados. Teniendo en cuenta que el inventario debe ser mantenido por las funciones pertinentes, puede verse como un conjunto de inventarios dinámicos, como inventarios de activos de información, hardware, software, máquinas virtuales (VM), instalaciones, personal, competencia, capacidades y registros.

Cada activo debe clasificarse de acuerdo con la clasificación de la información (ver5.12) asociado a ese activo.

La granularidad del inventario de información y otros activos asociados debe estar en un nivel apropiado para las necesidades de la organización. A veces, no es factible documentar instancias específicas de activos en el ciclo de vida de la información debido a la naturaleza del activo. Un ejemplo de un activo de corta duración es una instancia de VM cuyo ciclo de vida puede ser de corta duración.

Propiedad

Para la información identificada y otros activos asociados, la propiedad del activo debe asignarse a un individuo o grupo y debe identificarse la clasificación (ver5.12 ,5.13). Debe implementarse un proceso para garantizar la asignación oportuna de la propiedad de los activos. La propiedad debe asignarse cuando se crean los activos o cuando se transfieren los activos a la organización. La propiedad de los activos debe reasignarse según sea necesario cuando los propietarios actuales de los activos se van o cambian de puesto.

deberes del propietario

El propietario del activo debe ser responsable de la gestión adecuada de un activo durante todo el ciclo de vida del activo, asegurando que:

a) se inventarian la información y otros activos asociados;

b) la información y otros activos asociados estén debidamente clasificados y protegidos;

c) la clasificación se revisa periódicamente;

d) se enumeran y vinculan los componentes que respaldan los activos tecnológicos, como bases de datos, almacenamiento, componentes y subcomponentes de software;

e) requisitos para el uso aceptable de la información y otros activos asociados (ver5.10) están establecidos;

f) las restricciones de acceso correspondan con la clasificación y que sean efectivas y se revisen periódicamente;

g) la información y otros activos asociados, cuando se eliminen o eliminen, se manejen de manera segura y se eliminen del inventario;

h) están involucrados en la identificación y gestión de riesgos asociados con su(s) activo(s);

i) apoyan al personal que tiene los roles y responsabilidades de administrar su información.

Otra información

Los inventarios de información y otros activos asociados a menudo son necesarios para garantizar la protección efectiva de la información y pueden ser necesarios para otros fines, como salud y seguridad, seguros o razones financieras. Los inventarios de información y otros activos asociados también respaldan la gestión de riesgos, las actividades de auditoría, la gestión de vulnerabilidades, la respuesta a incidentes y la planificación de la recuperación.

Las tareas y responsabilidades se pueden delegar (por ejemplo, a un custodio que se ocupa de los activos diariamente), pero la persona o el grupo que las delegó sigue siendo responsable.

Puede ser útil designar grupos de información y otros activos asociados que actúan juntos para brindar un servicio particular. En este caso, el titular de este servicio es responsable de la prestación del servicio, incluida la explotación de sus activos.

Consulte ISO/IEC 19770-1 para obtener información adicional sobre la gestión de activos de tecnología de la información (TI). Consulte la norma ISO 55001 para obtener información adicional sobre la gestión de activos.

5.10 Uso aceptable de la información y otros activos asociados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gestión de activos #Información_protección	# Gobernanza_y_Ecosistema #Protección

Control

Deben identificarse, documentarse e implementarse reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

Propósito

Para garantizar que la información y otros activos asociados se protejan, utilicen y manejen adecuadamente.

Guia

El personal y los usuarios externos que utilicen o tengan acceso a la información de la organización y otros activos asociados deben conocer los requisitos de seguridad de la información para proteger y manejar la información de la organización y otros activos asociados. Deben ser responsables del uso que hagan de las instalaciones de procesamiento de información.

La organización debe establecer una política específica del tema sobre el uso aceptable de la información y otros activos asociados y comunicarla a cualquier persona que use o maneje información y otros activos asociados. La política específica del tema sobre el uso aceptable debe proporcionar una dirección clara sobre cómo se espera que las personas usen la información y otros activos asociados. La política específica del tema debe establecer:

a) comportamientos esperados e inaceptables de las personas desde una perspectiva de seguridad de la información;

b) uso permitido y prohibido de información y otros activos asociados;

c) las actividades de seguimiento que realiza la organización.

Deben elaborarse procedimientos de uso aceptable para todo el ciclo de vida de la información de acuerdo con su clasificación (ver5.12) y riesgos determinados. Se deben considerar los siguientes elementos:

a) restricciones de acceso que respaldan los requisitos de protección para cada nivel de clasificación;

b) mantenimiento de un registro de los usuarios autorizados de información y otros activos asociados;

c) protección de copias temporales o permanentes de información a un nivel consistente con la protección de la información original;

d) almacenamiento de activos asociados con la información de acuerdo con las especificaciones de los fabricantes (ver7.8);

e) marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos) para la atención del destinatario autorizado (ver7.10);

f) autorización de disposición de información y otros activos asociados y método (s) de eliminación admitido (ver8.10).

Otra información

Puede darse el caso de que los activos en cuestión no pertenezcan directamente a la organización, como los servicios de nube pública. El uso de dichos activos de terceros y cualquier activo de la organización asociado con dichos activos externos (por ejemplo, información, software) debe identificarse como aplicable y controlarse, por ejemplo, a través de acuerdos con proveedores de servicios en la nube. También se debe tener cuidado cuando se utiliza un entorno de trabajo colaborativo.

5.11 Devolución de bienes

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Asset_manage-mento	# Proteccion

Control

El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

Propósito

Para proteger los activos de la organización como parte del proceso de cambio o terminación de empleo, contrato o acuerdo.

Guia

El proceso de cambio o terminación debe formalizarse para incluir la devolución de todos los activos físicos y electrónicos emitidos anteriormente que sean propiedad de la organización o estén encomendados a ella.

En los casos en que el personal y otras partes interesadas compren el equipo de la organización o usen su propio equipo personal, se deben seguir los procedimientos para garantizar que toda la información relevante sea rastreada y transferida a la organización y eliminada de manera segura del equipo (ver7.14).

En los casos en que el personal y otras partes interesadas tengan conocimientos que sean importantes para las operaciones en curso, esa información debe documentarse y transferirse a la organización.

Durante el período de notificación y posteriormente, la organización debe evitar la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) por parte del personal bajo notificación de terminación.

La organización debe identificar y documentar claramente toda la información y otros activos asociados que se devolverán, que pueden incluir:

a) dispositivos de punto extremo de usuario;

b) dispositivos portátiles de almacenamiento;

c) equipo especializado;

d) hardware de autenticación (por ejemplo, llaves mecánicas, tokens físicos y tarjetas inteligentes) para sistemas de información, sitios y archivos físicos;

e) copias físicas de la información.

Otra información

Puede ser difícil devolver la información que se tiene sobre los activos que no son propiedad de la organización. En tales casos, es necesario restringir el uso de la información utilizando otros controles de seguridad de la información, como la gestión de derechos de acceso (5.18) o uso de criptografía (8.24).

5.12 Clasificación de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	#Información_protección	# Proteccion # Defensa

Control

La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

Propósito

Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.

Guia

La organización debe establecer una política específica de un tema sobre la clasificación de la información y comunicarla a todas las partes interesadas pertinentes.

La organización debe tener en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.

Las clasificaciones y los controles de protección asociados para la información deben tener en cuenta las necesidades comerciales para compartir o restringir la información, proteger la integridad de la información y garantizar la disponibilidad, así como los requisitos legales relacionados con la confidencialidad, integridad o disponibilidad de la información. Los activos distintos de la información también pueden clasificarse de acuerdo con la clasificación de la información, que se almacena, procesa o maneja o protege de otro modo por el activo.

Los propietarios de la información deben ser responsables de su clasificación.

El esquema de clasificación debe incluir convenciones para la clasificación y criterios para la revisión de la clasificación a lo largo del tiempo. Los resultados de la clasificación deben actualizarse de acuerdo con los cambios del valor, la sensibilidad y la criticidad de la información a lo largo de su ciclo de vida.

El esquema debe estar alineado con la política específica del tema sobre el control de acceso (ver5.1) y debe ser capaz de abordar las necesidades comerciales específicas de la organización.

La clasificación puede ser determinada por el nivel de impacto que el compromiso de la información tendría para la organización. Cada nivel definido en el esquema debe recibir un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.

El esquema debe ser consistente en toda la organización e incluirse en sus procedimientos para que todos clasifiquen la información y otros activos asociados aplicables de la misma manera. De esta manera, todos tienen un entendimiento común de los requisitos de protección y aplican la protección adecuada.

El esquema de clasificación utilizado dentro de la organización puede ser diferente de los esquemas utilizados por otras organizaciones, incluso si los nombres de los niveles son similares. Además, la información que se mueve entre

las organizaciones pueden variar en clasificación dependiendo de su contexto en cada organización, incluso si sus esquemas de clasificación son idénticos. Por lo tanto, los acuerdos con otras organizaciones que incluyen el intercambio de información deben incluir procedimientos para identificar la clasificación de esa información y para interpretar los niveles de clasificación de otras organizaciones. La correspondencia entre diferentes esquemas se puede determinar buscando la equivalencia en los métodos de manejo y protección asociados.

Otra información

La clasificación brinda a las personas que manejan información una indicación concisa de cómo manejarla y protegerla. La creación de grupos de información con necesidades de protección similares y la especificación de procedimientos de seguridad de la información que se aplican a toda la información de cada grupo facilita esto. Este enfoque reduce la necesidad de una evaluación de riesgos caso por caso y un diseño personalizado de los controles.

La información puede dejar de ser sensible o crítica después de un cierto período de tiempo. Por ejemplo, cuando la información se ha hecho pública, ya no tiene requisitos de confidencialidad pero aún puede requerir protección para sus propiedades de integridad y disponibilidad. Estos aspectos deben tenerse en cuenta, ya que la sobreclasificación puede llevar a la implementación de controles innecesarios que resulten en gastos adicionales o, por el contrario, la subclasificación puede llevar a controles insuficientes para proteger la información de compromisos.

A modo de ejemplo, un esquema de clasificación de la confidencialidad de la información puede basarse en los cuatro niveles siguientes:

a) la divulgación no causa daño;

b) la divulgación causa un daño reputacional menor o un impacto operativo menor;

c) la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos comerciales;

d) la divulgación tiene un impacto grave en los objetivos comerciales a largo plazo o pone en riesgo la supervivencia de la organización.

5.13 Etiquetado de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Información_ proteccion	# Defensa # Proteccion

Control

Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.

Propósito

Facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.

Guia

Los procedimientos para el etiquetado de la información deben cubrir la información y otros activos asociados en todos los formatos. El etiquetado debe reflejar el esquema de clasificación establecido en5.12 . Las etiquetas deben ser fácilmente reconocibles. Los procedimientos deben brindar orientación sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a la información o cómo se manejan los activos según los tipos de medios de almacenamiento. Los procedimientos pueden definir:

a) casos en los que se omite el etiquetado (p. ej., etiquetado de información no confidencial para reducir la carga de trabajo);

b) cómo etiquetar la información enviada o almacenada en medios electrónicos o físicos, o cualquier otro formato;

c) cómo manejar los casos en los que el etiquetado no es posible (por ejemplo, debido a restricciones técnicas).

Los ejemplos de técnicas de etiquetado incluyen:

a) etiquetas físicas;

b) encabezados y pies de página;

c) metadatos;

d) marca de agua;

e) sellos de goma.

La información digital debe utilizar metadatos para identificar, gestionar y controlar la información, especialmente en lo que respecta a la confidencialidad. Los metadatos también deben permitir una búsqueda eficiente y correcta de información. Los metadatos deben facilitar que los sistemas interactúen y tomen decisiones en función de las etiquetas de clasificación asociadas.

Los procedimientos deben describir cómo adjuntar metadatos a la información, qué etiquetas usar y cómo se deben manejar los datos, de acuerdo con el modelo de información y la arquitectura de TIC de la organización.

Los sistemas deben agregar metadatos adicionales relevantes cuando procesan información según sus propiedades de seguridad de la información.

El personal y otras partes interesadas deben conocer los procedimientos de etiquetado. Todo el personal debe recibir la capacitación necesaria para garantizar que la información se etiquete correctamente y se manipule en consecuencia.

Los resultados de los sistemas que contienen información clasificada como confidencial o crítica deben llevar una etiqueta de clasificación adecuada.

Otra información

El etiquetado de la información clasificada es un requisito clave para el intercambio de información.

Otros metadatos útiles que se pueden adjuntar a la información son qué proceso organizacional creó la información y en qué momento.

El etiquetado de la información y otros activos asociados a veces puede tener efectos negativos. Los activos clasificados pueden ser más fáciles de identificar por parte de actores maliciosos para un posible uso indebido.

Algunos sistemas no etiquetan archivos individuales o registros de bases de datos con su clasificación, pero protegen toda la información al más alto nivel de clasificación de cualquier información que contenga o que se le permita contener. Es habitual en dichos sistemas determinar y luego etiquetar la información cuando se exporta.

5.14 Transferencia de información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gestión de activos # Información_protección	# Proteccion

Control

Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

Propósito

Para mantener la seguridad de la información transferida dentro de una organización y con cualquier parte externa interesada.

Guia

General

La organización debe establecer y comunicar una política específica del tema sobre la transferencia de información a todas las partes interesadas relevantes. Las reglas, procedimientos y acuerdos para proteger la información en tránsito deben reflejar la clasificación de la información involucrada. Cuando se transfiera información entre la organización y terceros, se deben establecer y mantener acuerdos de transferencia (incluida la autenticación del destinatario) para proteger la información en todas las formas en tránsito (ver 5.10).

La transferencia de información puede ocurrir a través de transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal.

Para todo tipo de transferencia de información, las reglas, procedimientos y acuerdos deben incluir:

a) controles diseñados para proteger la información transferida de la intercepción, el acceso no autorizado, la copia, la modificación, el enrutamiento incorrecto, la destrucción y la denegación de servicio, incluidos los niveles de control de acceso acordes con la clasificación de la información involucrada y cualquier control especial que se requiera para proteger la información confidencial , como el uso de técnicas criptográficas (ver 8.24);

b) controles para garantizar la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito;

c) identificación de los contactos apropiados relacionados con la transferencia, incluidos los propietarios de la información, los propietarios del riesgo, los oficiales de seguridad y los custodios de la información, según corresponda;

d) responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de medios físicos de almacenamiento o datos;

e) uso de un sistema de etiquetado acordado para información sensible o crítica, asegurando que el significado de las etiquetas se entienda de inmediato y que la información esté debidamente protegida (ver 5.13);

f) confiabilidad y disponibilidad del servicio de transferencia;

g) la política o directrices específicas del tema sobre el uso aceptable de las instalaciones de transferencia de información (ver 5.10);

h) pautas de retención y eliminación para todos los registros comerciales, incluidos los mensajes;

NOTA Pueden existir leyes y reglamentos locales con respecto a la retención y eliminación de registros comerciales.

i) la consideración de cualquier otro requisito legal, estatutario, reglamentario y contractual relevante (ver 5.31 , 5.32 , 5.33 , 5.34) relacionados con la transferencia de información (por ejemplo, requisitos para las firmas electrónicas).

Transferencia electronica

Las reglas, los procedimientos y los acuerdos también deben considerar los siguientes elementos al utilizar las instalaciones de comunicación electrónica para la transferencia de información:

a) detección y protección contra malware que puede transmitirse mediante el uso de comunicaciones electrónicas (ver 8.7);

b) protección de la información electrónica sensible comunicada que se encuentra en forma de archivo adjunto;

c) prevención contra el envío de documentos y mensajes en las comunicaciones a la dirección o número equivocado;

d) obtener aprobación antes de utilizar servicios públicos externos, como mensajería instantánea, redes sociales, uso compartido de archivos o almacenamiento en la nube;

e) niveles más fuertes de autenticación al transferir información a través de redes de acceso público;

f) restricciones asociadas con las instalaciones de comunicación electrónica (p. ej., impedir el reenvío automático de correo electrónico a direcciones de correo externas);

g) advertir al personal y otras partes interesadas que no envíen servicios de mensajes cortos (SMS) o mensajes instantáneos con información crítica ya que estos pueden ser leídos en lugares públicos (y por lo tanto por personas no autorizadas) o almacenados en dispositivos no protegidos adecuadamente;

h) asesorar al personal y otras partes interesadas sobre los problemas del uso de máquinas o servicios de fax, a saber:

1) acceso no autorizado a los almacenes de mensajes incorporados para recuperar mensajes;

2) programación deliberada o accidental de máquinas para enviar mensajes a números específicos.

Transferencia de medios de almacenamiento físico

Al transferir medios físicos de almacenamiento (incluido el papel), las reglas, los procedimientos y los acuerdos también deben incluir:

a) responsabilidades de control y notificación de la transmisión, despacho y recepción;

b) asegurar el correcto direccionamiento y transporte del mensaje;

c) embalaje que proteja el contenido de cualquier daño físico que pueda surgir durante el tránsito y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protegiendo contra cualquier factor ambiental que pueda reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o la radiación electromagnética. campos; utilizar normas técnicas mínimas para el embalaje y la transmisión (por ejemplo, el uso de sobres opacos);

d) una lista de mensajeros confiables autorizados acordados por la gerencia;

e) estándares de identificación del mensajero;

f) dependiendo del nivel de clasificación de la información en los medios de almacenamiento a ser transportados, usar controles a prueba de manipulaciones o inviolables (por ejemplo, bolsas, contenedores);

g) procedimientos para verificar la identificación de los mensajeros;

h) lista aprobada de terceros que prestan servicios de transporte o mensajería según la clasificación de la información;

i) mantener registros para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar la lista de destinatarios autorizados, los tiempos de transferencia a los custodios de tránsito y la recepción en destino.

transferencia verbal

Para proteger la transferencia verbal de información, se debe recordar al personal y otras partes interesadas que deben:

a) no tener conversaciones verbales confidenciales en lugares públicos o por canales de comunicación inseguros, ya que pueden ser escuchadas por personas no autorizadas;

b) no deje mensajes que contengan información confidencial en contestadores automáticos o mensajes de voz, ya que estos pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta;

c) ser proyectado al nivel apropiado para escuchar la conversación;

d) asegurarse de que se implementen los controles de sala adecuados (p. ej., insonorización, puertas cerradas);

e) comenzar cualquier conversación delicada con un descargo de responsabilidad para que los presentes sepan el nivel de clasificación y los requisitos de manejo de lo que están a punto de escuchar.

Otra información

Ninguna otra información.

5.15 Control de acceso

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información.

Propósito

Para garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Guia

Los propietarios de la información y otros activos asociados deben determinar la seguridad de la información y los requisitos comerciales relacionados con el control de acceso. Debe definirse una política de control de acceso específica del tema que tenga en cuenta estos requisitos y debe comunicarse a todas las partes interesadas relevantes.

Estos requisitos y la política específica del tema deben considerar lo siguiente:

a) determinar qué entidades requieren qué tipo de acceso a la información y otros activos asociados;

b) seguridad de las aplicaciones (ver8.26);

c) acceso físico, que debe estar respaldado por controles de entrada físicos apropiados (ver7.2 ,7.3 , 7.4);

d) diseminación y autorización de la información (por ejemplo, el principio de necesidad de saber) y niveles de seguridad de la información y clasificación de la información (ver5.10 ,5.12 ,5.13);

e) restricciones al acceso privilegiado (ver8.2);

f) segregación de funciones (ver5.3);

g) la legislación, los reglamentos y las obligaciones contractuales pertinentes con respecto a la limitación del acceso a datos o servicios (ver5.31 ,5.32 ,5.33 ,5.34 ,8.3);

h) segregación de las funciones de control de acceso (por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso);

i) autorización formal de solicitudes de acceso (ver5.16 y5.18);

j) la gestión de los derechos de acceso (ver5.18);

k) registro (ver8.15).

Las reglas de control de acceso deben implementarse definiendo y mapeando los derechos y restricciones de acceso apropiados para las entidades relevantes (ver5.16). Una entidad puede representar tanto a un usuario humano como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio). Para simplificar la gestión del control de acceso, se pueden asignar roles específicos a grupos de entidades.

Se debe tener en cuenta lo siguiente al definir e implementar reglas de control de acceso:

a) coherencia entre los derechos de acceso y la clasificación de la información;

b) coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad del perímetro físico;

c) considerar todos los tipos de conexiones disponibles en entornos distribuidos para que las entidades solo tengan acceso a la información y otros activos asociados, incluidas las redes y los servicios de red, que están autorizadas a usar;

d) considerar cómo se pueden reflejar los elementos o factores relevantes para el control de acceso dinámico.

Otra información

A menudo se utilizan principios generales en el contexto del control de acceso. Dos de los principios más utilizados son:

a) necesidad de saber: una entidad solo tiene acceso a la información que esa entidad requiere para realizar sus tareas (diferentes tareas o roles significan diferente información de necesidad de saber y, por lo tanto, diferentes perfiles de acceso);

b) necesidad de uso: a una entidad solo se le asigna acceso a la infraestructura de tecnología de la información cuando existe una necesidad clara.

Se debe tener cuidado al especificar reglas de control de acceso para considerar:

a) establecer reglas basadas en la premisa del privilegio mínimo, “En general, todo está prohibido a menos que esté expresamente permitido”, en lugar de la regla más débil, “En general, todo está permitido a menos que esté expresamente prohibido”;

b) cambios en las etiquetas de información (ver5.13) que son iniciados automáticamente por las instalaciones de procesamiento de información y aquellos iniciados a discreción de un usuario;

c) cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos iniciados por un administrador;

d) cuándo definir y revisar periódicamente la aprobación.

Las reglas de control de acceso deben estar respaldadas por procedimientos documentados (ver5.16 ,5.17 ,5.18 ,8.2 ,8.3 ,8.4 , 8.5 ,8.18) y responsabilidades definidas (ver5.2 ,5.17).

Hay varias formas de implementar el control de acceso, como MAC (control de acceso obligatorio), DAC (control de acceso discrecional), RBAC (control de acceso basado en roles) y ABAC (control de acceso basado en atributos).

Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúa accesos anteriores o valores de entorno específicos). Las reglas de control de acceso se pueden implementar en diferentes granularidades, que van desde cubrir redes o sistemas completos hasta campos de datos específicos y también pueden considerar propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y cómo se define el control de acceso granular pueden tener un impacto significativo en los costos. Reglas más estrictas y más granularidad generalmente conducen a un costo más alto. Los requisitos comerciales y las consideraciones de riesgo deben usarse para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.

5.16 Gestión de identidad

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

Se debe gestionar el ciclo de vida completo de las identidades.

Propósito

Permitir la identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.

Guia

Los procesos utilizados en el contexto de la gestión de la identidad deben garantizar que:

a) para las identidades asignadas a personas, una identidad específica solo se vincula a una sola persona para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica;

b) las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por razones comerciales u operativas y están sujetas a aprobación y documentación específicas;

c) las identidades asignadas a entidades no humanas están sujetas a una aprobación segregada adecuada y a una supervisión continua independiente;

d) las identidades se deshabilitan o eliminan de manera oportuna si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan, o si la persona vinculada a una identidad ha dejado la organización o ha cambiado de función);

e) en un dominio específico, una sola identidad se mapea a una sola entidad, [es decir, se evita el mapeo de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)];

f) se mantienen registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación.

La organización debe contar con un proceso de soporte para manejar los cambios en la información relacionada con las identidades de los usuarios. Estos procesos pueden incluir la reverificación de documentos confiables relacionados con una persona.

Al utilizar identidades proporcionadas o emitidas por terceros (p. ej., credenciales de redes sociales), la organización debe asegurarse de que las identidades de terceros brinden el nivel de confianza requerido y que los riesgos asociados se conozcan y se traten adecuadamente. Esto puede incluir controles relacionados con terceros (ver5.19), así como los controles relacionados con la información de autenticación asociada (ver5.17).

Otra información

Proporcionar o revocar el acceso a la información y otros activos asociados suele ser un procedimiento de varios pasos:

a) confirmar los requisitos comerciales para establecer una identidad;

b) verificar la identidad de una entidad antes de asignarles una identidad lógica;

c) establecer una identidad;

d) configurar y activar la identidad. Esto también incluye la configuración y configuración inicial de los servicios de autenticación relacionados;

e) otorgar o revocar derechos de acceso específicos a la identidad, con base en las decisiones de autorización o derecho correspondientes (ver5.18).

5.17 Información de autenticación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

Propósito

Para garantizar la autenticación adecuada de la entidad y evitar fallas en los procesos de autenticación.

Guia

Asignación de información de autenticación

El proceso de asignación y gestión debe garantizar que:

a) las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción como información de autenticación secreta temporal no se pueden adivinar y son únicos para cada persona, y los usuarios deben cambiarlos después del primer uso;

b) se establecen procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación nueva, de reemplazo o temporal;

c) la información de autenticación, incluida la información de autenticación temporal, se transmite a los usuarios de manera segura (por ejemplo, a través de un canal autenticado y protegido) y se evita el uso de mensajes de correo electrónico sin protección (texto claro) para este propósito;

d) los usuarios acusan recibo de la información de autenticación;

e) la información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software;

f) se mantienen registros de eventos significativos relacionados con la asignación y gestión de la información de autenticación y se garantiza su confidencialidad, y se aprueba el método de mantenimiento de registros (p. ej. utilizando una herramienta de bóveda de contraseñas aprobada).

Responsabilidades del usuario

Cualquier persona que tenga acceso o utilice información de autenticación debe ser advertida de que se asegure de que:

a) la información de autenticación secreta, como las contraseñas, se mantiene confidencial. La información de autenticación secreta personal no debe compartirse con nadie. La información de autenticación secreta utilizada en el contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales se comparte únicamente con personas autorizadas;

b) la información de autenticación afectada o comprometida se cambia inmediatamente después de la notificación o cualquier otra indicación de un compromiso;

c) cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas seguras de acuerdo con las recomendaciones de las mejores prácticas, por ejemplo:

1) las contraseñas no se basan en nada que otra persona pueda adivinar u obtener fácilmente utilizando información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento);

2) las contraseñas no se basan en palabras del diccionario o combinaciones de las mismas;

3) use frases de contraseña fáciles de recordar e intente incluir caracteres alfanuméricos y especiales;

4) las contraseñas tienen una longitud mínima;

d) las mismas contraseñas no se utilizan en distintos servicios y sistemas;

e) la obligación de seguir estas reglas también está incluida en los términos y condiciones de empleo (ver 6.2).

Sistema de gestión de contraseñas

Cuando se utilizan contraseñas como información de autenticación, el sistema de administración de contraseñas debe:

a) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para abordar los errores de entrada;

b) aplicar contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas [ver c) de "Responsabilidades del usuario];

c) obligar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión;

d) hacer cumplir los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad, o al terminar o cambiar de empleo cuando un usuario tiene contraseñas conocidas para identidades que permanecen activas (por ejemplo, identidades compartidas);

e) evitar la reutilización de contraseñas anteriores;

f) evitar el uso de contraseñas de uso común y nombres de usuario comprometidos, combinaciones de contraseñas de sistemas pirateados;

g) no mostrar contraseñas en la pantalla cuando se ingresan;

h) almacenar y transmitir contraseñas en forma protegida.

El cifrado y el hashing de contraseñas deben realizarse de acuerdo con las técnicas criptográficas aprobadas para contraseñas (ver8.24).

Otra información

Las contraseñas o frases de contraseña son un tipo de información de autenticación de uso común y son un medio común para verificar la identidad de un usuario. Otros tipos de información de autenticación son claves criptográficas, datos almacenados en tokens de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación y datos biométricos, como escaneos de iris o huellas dactilares. Se puede encontrar información adicional en la serie ISO/IEC 24760.

Requerir cambios frecuentes de contraseñas puede ser problemático porque los usuarios pueden molestarse por los cambios frecuentes, olvidar nuevas contraseñas, anotarlas en lugares inseguros o elegir contraseñas no seguras. La provisión de inicio de sesión único (SSO) u otras herramientas de gestión de autenticación (por ejemplo, bóvedas de contraseñas) reduce la cantidad de información de autenticación que los usuarios deben proteger y, por lo tanto, puede aumentar la eficacia de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de información de autenticación.

Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario. En tales casos, a), c) yd) del "Sistema de gestión de contraseñas" no se aplican.

5.18 Derechos de acceso

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.

Propósito

Para garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos comerciales.

Guia

Concesión y revocación de los derechos de acceso

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico otorgados a la identidad autenticada de una entidad debe incluir:

a) obtener autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados (ver5.9). La aprobación por separado de los derechos de acceso por parte de la gerencia también puede ser apropiada;

b) considerando los requisitos comerciales y la política y las reglas específicas del tema de la organización sobre el control de acceso;

c) considerar la segregación de funciones, incluida la segregación de las funciones de aprobación e implementación de los derechos de acceso y la separación de funciones en conflicto;

d) garantizar que los derechos de acceso se eliminen cuando alguien no necesite acceder a la información y otros activos asociados, en particular garantizar que los derechos de acceso de los usuarios que han dejado la organización se eliminen de manera oportuna;

e) considerar otorgar derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de vencimiento, en particular para el personal temporal o el acceso temporal requerido por el personal;

f) verificar que el nivel de acceso otorgado esté de acuerdo con las políticas específicas del tema sobre control de acceso (ver5.15) y es coherente con otros requisitos de seguridad de la información, como la segregación de funciones (ver5.3);

g) garantizar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que se completen con éxito los procedimientos de autorización;

h) mantener un registro central de los derechos de acceso otorgados a un identificador de usuario (ID, lógico o físico) para acceder a la información y otros activos asociados;

i) modificar los derechos de acceso de los usuarios que han cambiado de rol o trabajo;

j) eliminar o ajustar los derechos de acceso físico y lógico, lo que puede hacerse mediante la eliminación, revocación o reemplazo de claves, información de autenticación, tarjetas de identificación o suscripciones;

k) mantener un registro de cambios en los derechos de acceso lógico y físico de los usuarios.

Revisión de los derechos de acceso

Las revisiones regulares de los derechos de acceso físico y lógico deben considerar lo siguiente:

a) los derechos de acceso de los usuarios después de cualquier cambio dentro de la misma organización (por ejemplo, cambio de trabajo, promoción, descenso) o terminación del empleo (ver6.1 para6.5);

b) autorizaciones de derechos de acceso privilegiado.

Consideración antes del cambio o terminación del empleo

Los derechos de acceso de un usuario a la información y otros activos asociados deben revisarse y ajustarse o eliminarse antes de cualquier cambio o terminación del empleo en función de la evaluación de factores de riesgo tales como:

a) si la terminación o cambio es iniciado por el usuario o por la administración y el motivo de la terminación;

b) las responsabilidades actuales del usuario;

c) el valor de los activos actualmente accesibles.

Otra información

Se debe considerar el establecimiento de roles de acceso de usuario en función de los requisitos comerciales que resumen una serie de derechos de acceso en perfiles de acceso de usuario típicos. Las solicitudes de acceso y las revisiones de los derechos de acceso se gestionan más fácilmente a nivel de dichos roles que a nivel de derechos particulares.

Se debe considerar la posibilidad de incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta acceder sin autorización (ver5.20 ,6.2 ,6.4 ,6.6).

En casos de rescisión iniciada por la gerencia, el personal descontento o los usuarios externos pueden corromper deliberadamente la información o sabotear las instalaciones de procesamiento de información. En los casos de personas que renuncian o son despedidas, pueden verse tentados a recopilar información para uso futuro.

La clonación es una forma eficiente para que las organizaciones asignen acceso a los usuarios. Sin embargo, debe hacerse con cuidado en función de los distintos roles identificados por la organización en lugar de simplemente clonar una identidad con todos los derechos de acceso asociados. La clonación tiene un riesgo inherente de dar lugar a derechos de acceso excesivos a la información y otros activos asociados.

5.19 Seguridad de la información en las relaciones con los proveedores

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# relación_proveedor-barcos_seguridad	# Gobernanza_y_Ecosistema # Protección ción

Control

Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Guia

La organización debe establecer y comunicar una política específica del tema sobre las relaciones con los proveedores a todas las partes interesadas pertinentes.

La organización debería identificar e implementar procesos y procedimientos para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Esto también debería aplicarse al uso que hace la organización de los recursos de los proveedores de servicios en la nube. Estos procesos y procedimientos deben incluir los que debe implementar la organización, así como aquellos que la organización requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor, tales como como:

a) identificar y documentar los tipos de proveedores (por ejemplo, servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización;

b) establecer cómo evaluar y seleccionar proveedores de acuerdo con la sensibilidad de la información, productos y servicios (por ejemplo, con análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones);

c) evaluar y seleccionar productos o servicios del proveedor que cuenten con controles adecuados de seguridad de la información y revisarlos; en particular, la precisión y exhaustividad de los controles implementados por el proveedor que aseguren la integridad de la información del proveedor y el procesamiento de la información y, por lo tanto, la seguridad de la información de la organización;

d) definir la información de la organización, los servicios TIC y la infraestructura física a la que los proveedores pueden acceder, monitorear, controlar o utilizar;

e) definir los tipos de componentes y servicios de infraestructura TIC proporcionados por los proveedores que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización;

f) evaluar y gestionar los riesgos de seguridad de la información asociados con:

1) el uso por parte de los proveedores de la información de la organización y otros activos asociados, incluidos los riesgos que se originan del personal del proveedor potencialmente malicioso;

2) mal funcionamiento o vulnerabilidades de los productos (incluidos los componentes y subcomponentes de software utilizados en estos productos) o servicios proporcionados por los proveedores;

g) monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por terceros y la validación del producto;

h) mitigar el incumplimiento de un proveedor, ya sea que este haya sido detectado a través del monitoreo o por otros medios;

i) el manejo de incidentes y contingencias asociadas con los productos y servicios del proveedor, incluidas las responsabilidades tanto de la organización como de los proveedores;

j) resiliencia y, si es necesario, medidas de recuperación y contingencia para garantizar la disponibilidad de la información del proveedor y el procesamiento de la información y, por lo tanto, la disponibilidad de la información de la organización;

k) concientización y capacitación para el personal de la organización que interactúa con el personal del proveedor con respecto a las reglas apropiadas de participación, políticas, procesos y procedimientos específicos del tema y comportamiento en función del tipo de proveedor y el nivel de acceso del proveedor a los sistemas e información de la organización;

l) administrar la transferencia necesaria de información, otros activos asociados y cualquier otra cosa que deba cambiarse y garantizar que la seguridad de la información se mantenga durante todo el período de transferencia;

m) requisitos para asegurar una terminación segura de la relación con el proveedor, incluyendo:

1) desaprovisionamiento de los derechos de acceso;

2) manejo de la información;

3) determinar la propiedad de la propiedad intelectual desarrollada durante el compromiso;

4) portabilidad de la información en caso de cambio de proveedor o internalización;

6) gestión de registros;

7) devolución de bienes;

8) eliminación segura de información y otros activos asociados;

9) requisitos continuos de confidencialidad;

n) nivel de seguridad del personal y seguridad física que se espera del personal y las instalaciones del proveedor.

Se deben considerar los procedimientos para continuar con el procesamiento de la información en caso de que el proveedor no pueda suministrar sus productos o servicios (por ejemplo, debido a un incidente, porque el proveedor ya no está en el negocio o ya no proporciona algunos componentes debido a los avances tecnológicos). para evitar cualquier retraso en la organización de productos o servicios de reemplazo (por ejemplo, identificar un proveedor alternativo por adelantado o utilizar siempre proveedores alternativos).

Otra información

En los casos en que no sea posible para una organización imponer requisitos a un proveedor, la organización debería:

a) considerar la orientación dada en este control al tomar decisiones sobre la elección de un proveedor y su producto o servicio;

b) implementar controles compensatorios según sea necesario con base en una evaluación de riesgos.

La información puede ser puesta en riesgo por proveedores con una gestión de seguridad de la información inadecuada. Deben determinarse y aplicarse controles para administrar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de confidencialidad o técnicas criptográficas. Otro ejemplo son los riesgos de protección de datos personales cuando el acuerdo con el proveedor implica la transferencia o el acceso a información a través de las fronteras. La organización debe ser consciente de que la responsabilidad legal o contractual de proteger la información sigue siendo de la organización.

Los riesgos también pueden ser causados por controles inadecuados de los componentes o servicios de infraestructura de TIC proporcionados por los proveedores. Los componentes o servicios defectuosos o vulnerables pueden provocar violaciones de la seguridad de la información en la organización o en otra entidad (p. ej., pueden provocar infecciones de malware, ataques u otros daños en entidades distintas a la organización).

Ver ISO/IEC 27036-2 para más detalles.

5.20 Abordar la seguridad de la información en los acuerdos con proveedores

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# relación_proveedor-barcos_seguridad	# Gobernanza_y_Ecosistema # Protección ción

Control

Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Guia

Los acuerdos con los proveedores deben establecerse y documentarse para garantizar que haya un entendimiento claro entre la organización y el proveedor con respecto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

Se puede considerar la inclusión de los siguientes términos en los acuerdos para satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se proporcionará o se accederá y los métodos para proporcionar o acceder a la información;

b) clasificación de la información de acuerdo con el esquema de clasificación de la organización (ver5.10 ,5.12 , 5.13);

c) mapeo entre el esquema de clasificación propio de la organización y el esquema de clasificación del proveedor;

d) los requisitos legales, estatutarios, reglamentarios y contractuales, incluida la protección de datos, el manejo de la información de identificación personal (PII), los derechos de propiedad intelectual y los derechos de autor y una descripción de cómo se garantizará que se cumplan;

e) obligación de cada parte contractual de implementar un conjunto de controles acordado, incluido el control de acceso, revisión del desempeño, monitoreo, informes y auditoría, y las obligaciones del proveedor de cumplir con los requisitos de seguridad de la información de la organización;

f) reglas de uso aceptable de la información y otros activos asociados, incluido el uso inaceptable si es necesario;

g) procedimientos o condiciones para la autorización y revocación de la autorización para el uso de la información de la organización y otros activos asociados por parte del personal del proveedor (por ejemplo, a través de una lista explícita del personal del proveedor autorizado para usar la información de la organización y otros activos asociados);

h) requisitos de seguridad de la información con respecto a la infraestructura TIC del proveedor; en particular, los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para que sirvan como base para los acuerdos de proveedores individuales basados en las necesidades comerciales de la organización y los criterios de riesgo;

i) indemnizaciones y remediación por incumplimiento de los requisitos por parte del contratista;

j) requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la remediación de incidentes);

k) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información (p. ej., para respuesta a incidentes, procedimientos de autorización);

l) disposiciones relevantes para la subcontratación, incluidos los controles que deben implementarse, como un acuerdo sobre el uso de subproveedores (por ejemplo, exigir que estén sujetos a las mismas obligaciones que el proveedor, exigir tener una lista de subcontratistas) proveedores y notificación ante cualquier cambio);

m) contactos relevantes, incluida una persona de contacto para cuestiones de seguridad de la información;

n) cualquier requisito de evaluación, cuando sea legalmente permisible, para el personal del proveedor, incluidas las responsabilidades de realizar los procedimientos de evaluación y notificación si la evaluación no se ha completado o si los resultados dan motivo de duda o preocupación;

o) los mecanismos de evidencia y aseguramiento de certificaciones de terceros para los requisitos de seguridad de la información relevantes relacionados con los procesos del proveedor y un informe independiente sobre la efectividad de los controles;

p) derecho a auditar los procesos y controles del proveedor relacionados con el contrato;

q) obligación del proveedor de entregar periódicamente un informe sobre la efectividad de los controles y acuerdo sobre la corrección oportuna de las cuestiones relevantes planteadas en el informe;

r) procesos de resolución de defectos y resolución de conflictos;

s) proporcionar respaldo alineado con las necesidades de la organización (en términos de frecuencia y tipo y ubicación de almacenamiento);

t) garantizar la disponibilidad de una instalación alternativa (es decir, un sitio de recuperación de desastres) que no esté sujeta a las mismas amenazas que la instalación principal y las consideraciones para los controles alternativos (controles alternativos) en caso de que fallen los controles principales;

u) tener un proceso de gestión de cambios que asegure la notificación previa a la organización y la posibilidad de que la organización no acepte cambios;

v) controles de seguridad física acordes con la clasificación de la información;

w) controles de transferencia de información para proteger la información durante la transferencia física o transmisión lógica;

x) cláusulas de rescisión al concluir el acuerdo, incluida la gestión de registros, la devolución de activos, la eliminación segura de información y otros activos asociados, y cualquier obligación de confidencialidad en curso;

y) provisión de un método para destruir de forma segura la información de la organización almacenada por el proveedor tan pronto como ya no sea necesaria;

z) asegurar, al final del contrato, la entrega del apoyo a otro proveedor oa la propia organización.

La organización debe establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorandos de entendimiento, acuerdos de intercambio de información) para realizar un seguimiento de adónde va su información. La organización también debe revisar, validar y actualizar regularmente sus acuerdos con partes externas para garantizar que aún sean necesarios y adecuados para su propósito con las cláusulas de seguridad de la información relevantes.

Otra información

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de proveedores. Por lo tanto, se debe tener cuidado de incluir todos los requisitos relevantes para abordar los riesgos de seguridad de la información.

Para obtener detalles sobre los acuerdos con los proveedores, consulte la serie ISO/IEC 27036. Para los acuerdos de servicios en la nube, consulte la serie ISO/IEC 19086.

5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# relación_proveedor-barcos_seguridad	# Gobernanza_y_Ecosistema # Protección ción

Control

Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Guia

Se deben considerar los siguientes temas para abordar la seguridad de la información dentro de la seguridad de la cadena de suministro de TIC, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de productos o servicios de TIC;

b) exigir que los proveedores de servicios de TIC propaguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro si subcontratan partes del servicio de TIC proporcionado a la organización;

c) exigir que los proveedores de productos TIC propaguen prácticas de seguridad adecuadas a lo largo de la cadena de suministro si estos productos incluyen componentes comprados o adquiridos de otros proveedores u otras entidades (por ejemplo, desarrolladores de software y proveedores de componentes de hardware subcontratados);

d) solicitar que los proveedores de productos TIC proporcionen información que describa los componentes de software utilizados en los productos;

e) solicitar que los proveedores de productos TIC proporcionen información que describa las funciones de seguridad implementadas de su producto y la configuración requerida para su operación segura;

f) implementar un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de TIC entregados cumplan con los requisitos de seguridad establecidos. Los ejemplos de dichos métodos de revisión de proveedores pueden incluir pruebas de penetración y prueba o validación de certificaciones de terceros para las operaciones de seguridad de la información del proveedor;

g) implementar un proceso para identificar y documentar los componentes del producto o servicio que son críticos para mantener la funcionalidad y, por lo tanto, requieren una mayor atención, escrutinio y seguimiento adicional cuando se construyen fuera de la organización, especialmente si el proveedor subcontrata aspectos de los componentes del producto o servicio a otros. proveedores;

h) obtener la seguridad de que los componentes críticos y su origen pueden rastrearse a lo largo de la cadena de suministro;

i) obtener la seguridad de que los productos TIC entregados funcionan como se espera sin características inesperadas o no deseadas;

j) implementar procesos para garantizar que los componentes de los proveedores sean genuinos y no se alteren sus especificaciones. Las medidas de ejemplo incluyen etiquetas antimanipulación, verificaciones hash criptográficas o firmas digitales. La supervisión del rendimiento fuera de las especificaciones puede ser un indicador de manipulación o falsificación. La prevención y detección de la manipulación debe implementarse durante varias etapas del ciclo de vida del desarrollo del sistema, incluido el diseño, el desarrollo, la integración, las operaciones y el mantenimiento;

k) obtener garantías de que los productos TIC alcancen los niveles de seguridad requeridos, por ejemplo, a través de una certificación formal o un esquema de evaluación como el Acuerdo de Reconocimiento de Criterios Comunes;

l) definir reglas para compartir información sobre la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores;

m) implementar procesos específicos para gestionar el ciclo de vida y la disponibilidad de los componentes TIC y los riesgos de seguridad asociados. Esto incluye gestionar los riesgos de que los componentes ya no estén disponibles debido a que los proveedores ya no están en el negocio o los proveedores ya no proporcionan estos componentes debido a los avances tecnológicos. Se debe considerar la identificación de un proveedor alternativo y el proceso para transferir el software y la competencia al proveedor alternativo.

Otra información

Las prácticas específicas de gestión de riesgos de la cadena de suministro de TIC se basan en las prácticas generales de seguridad de la información, calidad, gestión de proyectos e ingeniería de sistemas, pero no las reemplazan.

Se aconseja a las organizaciones que trabajen con los proveedores para comprender la cadena de suministro de las TIC y cualquier asunto que tenga un efecto importante en los productos y servicios que se proporcionan. La organización puede influir en las prácticas de seguridad de la información de la cadena de suministro de TIC dejando claro en los acuerdos con sus proveedores los asuntos que deben abordar otros proveedores en la cadena de suministro de TIC.

Las TIC deben adquirirse de fuentes acreditadas. La confiabilidad del software y el hardware es una cuestión de control de calidad. Si bien generalmente no es posible que una organización inspeccione los sistemas de control de calidad de sus proveedores, puede hacer juicios confiables basados en la reputación del proveedor.

La cadena de suministro de TIC, como se aborda aquí, incluye servicios en la nube.

Ejemplos de cadenas de suministro de TIC son:

a) aprovisionamiento de servicios en la nube, donde el proveedor de servicios en la nube depende de los desarrolladores de software, proveedores de servicios de telecomunicaciones, proveedores de hardware;

b) IoT, donde el servicio involucra a los fabricantes de dispositivos, los proveedores de servicios en la nube (por ejemplo, los operadores de la plataforma IoT), los desarrolladores de aplicaciones móviles y web, el proveedor de bibliotecas de software;

c) servicios de hospedaje, donde el proveedor se basa en mesas de servicio externas, incluidos los niveles de soporte primero, segundo y tercero.

Consulte ISO / IEC 27036-3 para obtener más detalles, incluida la guía de evaluación de riesgos.

Las etiquetas de identificación de software (SWID) también pueden ayudar a lograr una mejor seguridad de la información en la cadena de suministro, al proporcionar información sobre la procedencia del software. Ver ISO/IEC 19770-2 para más detalles.

5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# relación_proveedor-barcos_seguridad	# Gobernanza_y_Ecosistema # Protección ción # Defensa # Information_security_assurance

Control

La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.

Propósito

Mantener un nivel acordado de seguridad de la información y prestación de servicios en línea con los acuerdos con los proveedores.

Guia

El seguimiento, la revisión y la gestión de cambios de los servicios del proveedor deben garantizar que se cumplan los términos y condiciones de seguridad de la información de los acuerdos, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente y que los cambios en los servicios del proveedor o el estado comercial no afecten la prestación del servicio.

Esto debería implicar un proceso para gestionar la relación entre la organización y el proveedor para:

a) monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos;

b) controlar los cambios realizados por los proveedores, incluidos:

1) mejoras a los servicios actuales ofrecidos;

2) desarrollo de nuevas aplicaciones y sistemas;

3) modificaciones o actualizaciones de las políticas y procedimientos del proveedor;

4) controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad de la información;

c) monitorear los cambios en los servicios del proveedor, incluyendo:

1) cambios y mejoras a las redes;

2) uso de nuevas tecnologías;

3) adopción de nuevos productos o versiones o lanzamientos más nuevos;

4) nuevas herramientas y entornos de desarrollo;

5) cambios en la ubicación física de las instalaciones de servicio;

6) cambio de subproveedores;

7) subcontratación a otro proveedor;

d) revisar los informes de servicio producidos por el proveedor y organizar reuniones regulares de progreso según lo requieran los acuerdos;

e) realizar auditorías de proveedores y subproveedores, junto con la revisión de los informes de los auditores independientes, si están disponibles, y dar seguimiento a los problemas identificados;

f) proporcionar información sobre incidentes de seguridad de la información y revisar esta información según lo requieran los acuerdos y las pautas y procedimientos de apoyo;

g) revisar las pistas de auditoría del proveedor y los registros de eventos de seguridad de la información, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado;

h) responder y gestionar cualquier evento o incidente de seguridad de la información identificado;

i) identificar vulnerabilidades de seguridad de la información y gestionarlas;

j) revisar los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores;

k) asegurar que el proveedor mantenga suficiente capacidad de servicio junto con planes viables diseñados para asegurar que los niveles de continuidad del servicio acordados se mantengan después de fallas importantes en el servicio o desastres (ver5.29 ,5.30 ,5.35 ,5.36 ,8.14);

l) asegurar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos;

m) evaluar periódicamente que los proveedores mantienen niveles adecuados de seguridad de la información.

La responsabilidad de administrar las relaciones con los proveedores debe asignarse a un individuo o equipo designado. Deben estar disponibles suficientes habilidades técnicas y recursos para monitorear que se cumplan los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Se deben tomar las acciones apropiadas cuando se observen deficiencias en la prestación del servicio.

Otra información

Ver ISO/IEC 27036-3 para más detalles.

5.23 Seguridad de la información para el uso de servicios en la nube

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# relación_proveedor-barcos_seguridad	# Gobernanza_y_ Ecosistema # Protección ción

Control

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.

Propósito

Especificar y administrar la seguridad de la información para el uso de servicios en la nube.

Guia

La organización debe establecer y comunicar una política específica sobre el uso de los servicios en la nube a todas las partes interesadas relevantes.

La organización debe definir y comunicar cómo pretende gestionar los riesgos de seguridad de la información asociados con el uso de servicios en la nube. Puede ser una extensión o parte del enfoque existente sobre cómo una organización gestiona los servicios proporcionados por terceros (ver5.21 y5.22).

El uso de servicios en la nube puede implicar una responsabilidad compartida por la seguridad de la información y un esfuerzo de colaboración entre el proveedor del servicio en la nube y la organización que actúa como cliente del servicio en la nube. Es esencial que las responsabilidades tanto del proveedor de servicios en la nube como de la organización, que actúa como cliente del servicio en la nube, se definan e implementen de manera adecuada.

La organización debe definir:

a) todos los requisitos de seguridad de la información pertinentes asociados con el uso de los servicios en la nube;

b) criterios de selección del servicio en la nube y alcance del uso del servicio en la nube;

c) funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube;

d) qué controles de seguridad de la información gestiona el proveedor de servicios en la nube y cuáles gestiona la organización como cliente del servicio en la nube;

e) cómo obtener y utilizar las capacidades de seguridad de la información proporcionadas por el proveedor de servicios en la nube;

f) cómo obtener garantías sobre los controles de seguridad de la información implementados por los proveedores de servicios en la nube;

g) cómo administrar los controles, las interfaces y los cambios en los servicios cuando una organización utiliza múltiples servicios en la nube, particularmente de diferentes proveedores de servicios en la nube;

h) procedimientos para el manejo de incidentes de seguridad de la información que se produzcan en relación con el uso de los servicios en la nube;

i) su enfoque para monitorear, revisar y evaluar el uso continuo de los servicios en la nube para administrar los riesgos de seguridad de la información;

j) cómo cambiar o detener el uso de los servicios en la nube, incluidas las estrategias de salida para los servicios en la nube.

Los acuerdos de servicios en la nube a menudo están predefinidos y no están abiertos a negociación. Para todos los servicios en la nube, la organización debe revisar los acuerdos de servicios en la nube con los proveedores de servicios en la nube. Un acuerdo de servicio en la nube debe abordar los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la organización, con objetivos de nivel de servicio en la nube y objetivos cualitativos de servicio en la nube apropiados. La organización también debería realizar evaluaciones de riesgos relevantes para identificar

los riesgos asociados con el uso del servicio en la nube. Cualquier riesgo residual relacionado con el uso del servicio en la nube debe ser claramente identificado y aceptado por la gerencia adecuada de la organización.

Un acuerdo entre el proveedor de servicios en la nube y la organización, que actúa como cliente del servicio en la nube, debe incluir las siguientes disposiciones para la protección de los datos de la organización y la disponibilidad de los servicios:

a) proporcionar soluciones basadas en estándares aceptados por la industria para la arquitectura y la infraestructura;

b) administrar los controles de acceso del servicio en la nube para cumplir con los requisitos de la organización;

c) implementar soluciones de protección y monitoreo de malware;

d) procesar y almacenar la información confidencial de la organización en ubicaciones aprobadas (p. ej., un país o una región en particular) o dentro o sujeto a una jurisdicción en particular;

e) brindar soporte dedicado en caso de un incidente de seguridad de la información en el entorno del servicio en la nube;

f) garantizar que se cumplan los requisitos de seguridad de la información de la organización en caso de que se subcontraten servicios en la nube a un proveedor externo (o se prohíba la subcontratación de servicios en la nube);

g) apoyar a la organización en la recopilación de evidencia digital, teniendo en cuenta las leyes y regulaciones para evidencia digital en diferentes jurisdicciones;

h) proporcionar soporte y disponibilidad de servicios apropiados durante un período de tiempo apropiado cuando la organización desea salir del servicio en la nube;

i) proporcionar la copia de seguridad necesaria de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por la organización, actuando como cliente del servicio en la nube;

j) proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad de la organización, actuando como cliente del servicio en la nube, cuando se solicite durante la prestación del servicio o al finalizar el servicio.

La organización, actuando como cliente del servicio en la nube, debe considerar si el acuerdo debe exigir a los proveedores de servicios en la nube que proporcionen una notificación previa antes de que se realicen cambios sustanciales que afecten al cliente en la forma en que se entrega el servicio a la organización, incluidos:

a) cambios en la infraestructura técnica (p. ej., reubicación, reconfiguración o cambios en el hardware o el software) que afecten o modifiquen la oferta de servicios en la nube;

b) procesar o almacenar información en una nueva jurisdicción geográfica o legal;

c) uso de proveedores de servicios en la nube similares u otros subcontratistas (incluido el cambio de partes existentes o el uso de nuevas partes).

La organización que utiliza servicios en la nube debe mantener un estrecho contacto con sus proveedores de servicios en la nube. Estos contactos permiten el intercambio mutuo de información sobre la seguridad de la información para el uso de los servicios en la nube, incluido un mecanismo para que tanto el proveedor del servicio en la nube como la organización, que actúa como cliente del servicio en la nube, monitoreen cada característica del servicio e informen los incumplimientos de los compromisos contenidos en el acuerdos.

Otra información

Este control considera la seguridad en la nube desde la perspectiva del cliente del servicio en la nube.

Puede encontrar información adicional relacionada con los servicios en la nube en ISO/IEC 17788, ISO/IEC 17789 e ISO/IEC 22123-1. Los detalles relacionados con la portabilidad de la nube en apoyo de las estrategias de salida se pueden encontrar en ISO / IEC 19941. Los detalles relacionados con la seguridad de la información y los servicios de nube pública se describen en ISO / IEC 27017. Se describen los detalles relacionados con la protección de PII en nubes públicas que actúan como procesador de PII.

en ISO/IEC 27018. Las relaciones con los proveedores de servicios en la nube están cubiertas por ISO/IEC 27036-4 y los acuerdos de servicios en la nube y sus contenidos se tratan en la serie ISO/IEC 19086, con seguridad y privacidad específicamente cubiertas por ISO/IEC 19086- 4.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Confidencialidad # Integridad # Disponibilidad	#Responder #Recuperar	# Gobernanza # Information_security_event_management	# Defensa

Control

La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.

Propósito

Garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad de la información.

Guia

Funciones y responsabilidades

La organización debe establecer procesos apropiados de gestión de incidentes de seguridad de la información. Las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deben determinarse y comunicarse de manera efectiva a las partes interesadas internas y externas pertinentes.

Se debe considerar lo siguiente:

a) establecer un método común para reportar eventos de seguridad de la información, incluido el punto de contacto (ver 6.8);

b) establecer un proceso de gestión de incidentes para proporcionar a la organización la capacidad de gestionar incidentes de seguridad de la información, incluida la administración, documentación, detección, clasificación, priorización, análisis, comunicación y coordinación de las partes interesadas;

c) establecer un proceso de respuesta a incidentes para proporcionar a la organización la capacidad de evaluar, responder y aprender de los incidentes de seguridad de la información;

d) solo permitir que personal competente maneje los problemas relacionados con los incidentes de seguridad de la información dentro de la organización. Dicho personal debe contar con documentación de procedimientos y capacitación periódica;

e) establecer un proceso para identificar la capacitación, la certificación y el desarrollo profesional continuo necesarios para el personal de respuesta a incidentes.

Procedimientos de gestión de incidentes

Los objetivos para la gestión de incidentes de seguridad de la información deben acordarse con la gerencia y debe garantizarse que los responsables de la gestión de incidentes de seguridad de la información entiendan las prioridades de la organización para manejar los incidentes de seguridad de la información, incluido el marco de tiempo de resolución basado en las posibles consecuencias y gravedad. Se deben implementar procedimientos de gestión de incidentes para cumplir con estos objetivos y prioridades.

La gerencia debe asegurarse de que se cree un plan de gestión de incidentes de seguridad de la información considerando diferentes escenarios y se desarrollen e implementen procedimientos para las siguientes actividades:

a) evaluación de eventos de seguridad de la información según criterios de lo que constituye un incidente de seguridad de la información;

b) monitoreo (ver8.15 y8.16), detectar (ver8.16), clasificar (ver5.25), analizar e informar (ver6.8) de eventos e incidentes de seguridad de la información (por medios humanos o automáticos);

c) gestionar los incidentes de seguridad de la información hasta su conclusión, incluida la respuesta y el escalamiento (ver5.26), según el tipo y categoría del incidente, posible activación de gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación a partes interesadas internas y externas;

d) coordinación con partes interesadas internas y externas tales como autoridades, grupos de interés y foros externos, proveedores y clientes (ver5.5 y5.6);

e) registrar las actividades de gestión de incidentes;

f) manejo de evidencia (ver5.28);

g) análisis de causa raíz o procedimientos post-mortem;

h) identificación de las lecciones aprendidas y de las mejoras a los procedimientos de gestión de incidentes o controles de seguridad de la información en general que se requieran.

Procedimientos de notificación

Los procedimientos de notificación deben incluir:

a) acciones a tomar en caso de un evento de seguridad de la información (p. ej., tomar nota de todos los detalles pertinentes de inmediato, como el mal funcionamiento y los mensajes en pantalla, informar de inmediato al punto de contacto y solo tomar acciones coordinadas);

b) uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar incidentes de seguridad de la información;

c) procesos de retroalimentación adecuados para asegurar que aquellas personas que reporten eventos de seguridad de la información sean notificadas, en la medida de lo posible, de los resultados después de que el problema haya sido abordado y cerrado;

d) elaboración de informes de incidencias.

Cualquier requisito externo sobre la notificación de incidentes a las partes interesadas relevantes dentro del marco de tiempo definido (p. ej., requisitos de notificación de incumplimiento a los reguladores) debe tenerse en cuenta al implementar los procedimientos de gestión de incidentes.

Otra información

Los incidentes de seguridad de la información pueden trascender las fronteras organizacionales y nacionales. Para responder a tales incidentes, es beneficioso coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas, según corresponda.

En la serie ISO/IEC 27035 se proporciona una guía detallada sobre la gestión de incidentes de seguridad de la información.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective	# Confidencialidad # Integridad # Disponibilidad	# Detectar #Responder	# Information_security_event_management	# Defensa

Control

La organización debería evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.

Propósito

Para asegurar una categorización y priorización efectiva de los eventos de seguridad de la información.

Guia

Se debe acordar un esquema de categorización y priorización de incidentes de seguridad de la información para la identificación de las consecuencias y prioridad de un incidente. El esquema debe incluir los criterios para categorizar eventos como incidentes de seguridad de la información. El punto de contacto debe evaluar cada evento de seguridad de la información utilizando el esquema acordado.

El personal responsable de coordinar y responder a los incidentes de seguridad de la información debe realizar la evaluación y tomar una decisión sobre los eventos de seguridad de la información.

Los resultados de la evaluación y la decisión deben registrarse en detalle para fines de futura referencia y verificación.

Otra información

La serie ISO/IEC 27035 proporciona más orientación sobre la gestión de incidentes.

5.26 Respuesta a incidentes de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Confidencialidad # Integridad # Disponibilidad	#Responder #Recuperar	# Information_security_event_management	# Defensa

Control

Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Propósito

Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información.

Guia

La organización debe establecer y comunicar procedimientos sobre la respuesta a incidentes de seguridad de la información a todas las partes interesadas pertinentes.

Los incidentes de seguridad de la información deben ser respondidos por un equipo designado con la competencia requerida (ver5.24).

La respuesta debe incluir lo siguiente:

a) contener, si las consecuencias del incidente pueden extenderse, los sistemas afectados por el incidente;

b) recopilar evidencia (ver5.28) tan pronto como sea posible después de la ocurrencia;

c) escalamiento, según sea necesario, incluidas las actividades de gestión de crisis y posiblemente la invocación de planes de continuidad del negocio (ver5.29 y5.30);

d) garantizar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis;

e) comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a todas las partes interesadas internas y externas pertinentes siguiendo el principio de necesidad de saber;

f) coordinarse con partes internas y externas como autoridades, grupos y foros de interés externos, proveedores y clientes para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones;

g) una vez solucionado satisfactoriamente el incidente, cerrarlo formalmente y registrarlo;

h) realizar análisis forenses de seguridad de la información, según se requiera (ver5.28);

i) realizar un análisis posterior al incidente para identificar la causa raíz. Asegúrese de que esté documentado y comunicado de acuerdo con los procedimientos definidos (ver5.27);

j) identificar y gestionar las vulnerabilidades y debilidades de la seguridad de la información, incluidas las relacionadas con los controles que han causado, contribuido o fallado en prevenir el incidente.

Otra información

La serie ISO/IEC 27035 proporciona más orientación sobre la gestión de incidentes.

5.27 Aprendiendo de los incidentes de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Information_security_event_management	# Defensa

Control

El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.

Propósito

Para reducir la probabilidad o las consecuencias de futuros incidentes.

Guia

La organización debe establecer procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información.

La información obtenida de la evaluación de incidentes de seguridad de la información debe utilizarse para:

a) mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de incidentes (ver5.24);

b) identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad de la información de la organización y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares. Los mecanismos para habilitar eso incluyen recopilar, cuantificar y monitorear información sobre tipos de incidentes, volúmenes y costos;

c) mejorar la concienciación y la formación de los usuarios (véase6.3) proporcionando ejemplos de lo que puede suceder, cómo responder a tales incidentes y cómo evitarlos en el futuro.

Otra información

La serie ISO/IEC 27035 proporciona más orientación.

5.28 Recopilación de pruebas

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Detectar #Responder	# Information_security_event_management	# Defensa

Control

La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

Propósito

Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.

Guia

Se deben desarrollar y seguir procedimientos internos al tratar con evidencia relacionada con eventos de seguridad de la información con el propósito de acciones disciplinarias y legales. Se deben considerar los requisitos de las diferentes jurisdicciones para maximizar las posibilidades de admisión en las jurisdicciones relevantes.

En general, estos procedimientos para la gestión de pruebas deben proporcionar instrucciones para la identificación, recopilación, adquisición y conservación de pruebas de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y estado de los dispositivos (es decir, encendidos o apagados). Por lo general, las pruebas deben recopilarse de una manera que sea admisible en los tribunales de justicia nacionales correspondientes u otro foro disciplinario. Debería ser posible demostrar que:

a) los registros están completos y no han sido manipulados de ninguna manera;

b) las copias de las pruebas electrónicas probablemente sean idénticas a los originales;

c) cualquier sistema de información a partir del cual se hayan recopilado pruebas funcionaba correctamente en el momento en que se registraron las pruebas.

Cuando esté disponible, se debe buscar la certificación u otros medios relevantes de calificación del personal y las herramientas, para fortalecer el valor de la evidencia preservada.

La evidencia digital puede trascender los límites organizacionales o jurisdiccionales. En tales casos, se debe garantizar que la organización tenga derecho a recopilar la información requerida como evidencia digital.

Otra información

Cuando se detecta por primera vez un evento de seguridad de la información, no siempre es obvio si el evento resultará o no en una acción judicial. Por lo tanto, existe el peligro de que las pruebas necesarias se destruyan intencional o accidentalmente antes de darse cuenta de la gravedad del incidente. Es aconsejable involucrar asesoramiento legal o aplicación de la ley desde el principio en cualquier acción legal contemplada y recibir asesoramiento sobre las pruebas requeridas.

ISO/IEC 27037 proporciona definiciones y pautas para la identificación, recolección, adquisición y preservación de evidencia digital.

La serie ISO/IEC 27050 se ocupa del descubrimiento electrónico, que implica el procesamiento de información almacenada electrónicamente como prueba.

5.29 Seguridad de la información durante la interrupción

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Responder	# Continuidad	# Proteccion # Resiliencia

Control

La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

Propósito

Para proteger la información y otros activos asociados durante la interrupción.

Guia

La organización debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

Los planes deben desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos comerciales críticos luego de una interrupción o falla. La seguridad de la información debe restaurarse al nivel requerido y en los plazos requeridos.

La organización debe implementar y mantener:

a) controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad del negocio y continuidad de las TIC;

b) procesos para mantener los controles de seguridad de la información existentes durante la interrupción;

c) controles de compensación para los controles de seguridad de la información que no se pueden mantener durante la interrupción.

Otra información

En el contexto de la continuidad del negocio y la planificación de la continuidad de las TIC, puede ser necesario adaptar los requisitos de seguridad de la información según el tipo de interrupción, en comparación con las condiciones operativas normales. Como parte del análisis de impacto comercial y la evaluación de riesgos realizados dentro de la gestión de continuidad comercial, se deben considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad.

La información sobre los sistemas de gestión de la continuidad del negocio se puede encontrar en ISO 22301 e ISO 22313. Se puede encontrar más orientación sobre el análisis de impacto comercial (BIA) en ISO / TS 22317.

5.30 Preparación de las TIC para la continuidad del negocio

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Disponibilidad	# Responder	# Continuidad	# Resiliencia

Control

La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

Propósito

Para garantizar la disponibilidad de la información de la organización y otros activos asociados durante la interrupción.

Guia

La preparación de las TIC para la continuidad del negocio es un componente importante en la gestión de la continuidad del negocio y la gestión de la seguridad de la información para garantizar que los objetivos de la organización puedan seguir cumpliéndose durante la interrupción.

Los requisitos de continuidad de las TIC son el resultado del análisis de impacto empresarial (BIA). El proceso BIA debe utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo que resultan de la interrupción de las actividades comerciales que entregan productos y servicios. La magnitud y la duración del impacto resultante deben usarse para identificar actividades prioritarias a las que se les debe asignar un objetivo de tiempo de recuperación (RTO). Luego, el BIA debe determinar qué recursos se necesitan para apoyar las actividades priorizadas. También se debe especificar un RTO para estos recursos. Un subconjunto de estos recursos debería incluir servicios de TIC.

El BIA relacionado con los servicios de TIC se puede ampliar para definir los requisitos de rendimiento y capacidad de los sistemas de TIC y los objetivos de punto de recuperación (RPO) de la información necesaria para respaldar las actividades durante la interrupción.

Con base en los resultados del BIA y la evaluación de riesgos relacionados con los servicios de TIC, la organización debe identificar y seleccionar estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de la interrupción. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. Con base en las estrategias, los planes deben desarrollarse, implementarse y probarse para cumplir con el nivel de disponibilidad requerido de los servicios de TIC y en los plazos requeridos luego de la interrupción o falla de los procesos críticos.

La organización debe asegurarse de que:

a) existe una estructura organizativa adecuada para prepararse, mitigar y responder a una interrupción con el apoyo de personal con la responsabilidad, autoridad y competencia necesarias;

b) Los planes de continuidad de las TIC, incluidos los procedimientos de respuesta y recuperación que detallan cómo la organización planea gestionar una interrupción del servicio de TIC, son:

1) evaluado regularmente a través de ejercicios y pruebas;

2) aprobado por la gerencia;

c) Los planes de continuidad TIC incluyen la siguiente información de continuidad TIC:

1) especificaciones de rendimiento y capacidad para cumplir con los requisitos y objetivos de continuidad del negocio como se especifica en el BIA;

2) RTO de cada servicio TIC priorizado y los procedimientos para restaurar esos componentes;

3) RPO de los recursos TIC priorizados definidos como información y los procedimientos para restaurar la información.

Otra información

La gestión de la continuidad de las TIC constituye una parte clave de los requisitos de continuidad del negocio en relación con la disponibilidad para poder:

a) responder y recuperarse de la interrupción de los servicios de TIC, independientemente de la causa;

b) garantizar que la continuidad de las actividades prioritarias esté respaldada por los servicios de TIC requeridos;

c) responder antes de que ocurra una interrupción de los servicios de TIC, y al detectar al menos un incidente que pueda resultar en una interrupción de los servicios de TIC.

Puede encontrar más orientación sobre la preparación de las TIC para la continuidad del negocio en ISO / IEC 27031.

Puede encontrar más orientación sobre los sistemas de gestión de la continuidad del negocio en las normas ISO 22301 e ISO 22313.

Se puede encontrar más orientación sobre BIA en ISO / TS 22317.

5.31 Requisitos legales, estatutarios, reglamentarios y contractuales

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Legal_and_compli-ance	# Gobernanza_y_ Ecosistema # Protección ción

Control

Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.

Propósito

Asegurar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información.

Guia

General

Los requisitos externos, incluidos los requisitos legales, estatutarios, reglamentarios o contractuales, deben tenerse en cuenta cuando:

a) desarrollar políticas y procedimientos de seguridad de la información;

b) diseñar, implementar o cambiar los controles de seguridad de la información;

c) clasificar la información y otros activos asociados como parte del proceso para establecer requisitos de seguridad de la información para necesidades internas o para acuerdos con proveedores;

d) realizar evaluaciones de riesgos de seguridad de la información y determinar las actividades de tratamiento de riesgos de seguridad de la información;

e) determinar los procesos junto con las funciones y responsabilidades relacionadas con la seguridad de la información;

f) determinar los requisitos contractuales de los proveedores relevantes para la organización y el alcance del suministro de productos y servicios.

Legislación y reglamentos

La organización debería:

a) identificar toda la legislación y los reglamentos pertinentes a la seguridad de la información de la organización para conocer los requisitos para su tipo de negocio;

b) tomar en consideración el cumplimiento en todos los países relevantes, si la organización:

- realiza negocios en otros países;

- utiliza productos y servicios de otros países donde las leyes y reglamentos pueden afectar a la organización;

- transfiere información a través de fronteras jurisdiccionales donde las leyes y reglamentos pueden afectar a la organización;

c) revisar periódicamente la legislación y los reglamentos identificados para mantenerse al día con los cambios e identificar nueva legislación;

d) definir y documentar los procesos específicos y las responsabilidades individuales para cumplir con estos requisitos.

Criptografía

La criptografía es un área que a menudo tiene requisitos legales específicos. Se debe tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos pertinentes relacionados con los siguientes elementos:

a) restricciones a la importación o exportación de hardware y software informático para realizar funciones criptográficas;

b) restricciones a la importación o exportación de hardware y software informático que esté diseñado para tener funciones criptográficas añadidas;

c) restricciones en el uso de la criptografía;

d) métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a la información cifrada;

e) vigencia de firmas digitales, sellos y certificados.

Se recomienda buscar asesoramiento legal al garantizar el cumplimiento de la legislación y las reglamentaciones pertinentes, especialmente cuando la información cifrada o las herramientas criptográficas se mueven a través de las fronteras jurisdiccionales.

Contratos

Los requisitos contractuales relacionados con la seguridad de la información deben incluir los establecidos en:

a) contratos con clientes;

b) contratos con proveedores (ver5.20);

c) contratos de seguro.

Otra información

Ninguna otra información.

5.32 Derechos de propiedad intelectual

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	# Legal_and_compli-ance	# Gobernanza_y_ Ecosistema

Control

La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.

Propósito

Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

Guia

Se deben considerar las siguientes pautas para proteger cualquier material que pueda considerarse propiedad intelectual:

a) definir y comunicar una política específica sobre la protección de los derechos de propiedad intelectual;

b) publicar procedimientos para el cumplimiento de los derechos de propiedad intelectual que definan el uso conforme de software y productos de información;

c) adquirir software solo a través de fuentes conocidas y acreditadas, para garantizar que no se infrinjan los derechos de autor;

d) mantener registros de activos apropiados e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual;

e) mantener pruebas y evidencias de propiedad de licencias, manuales, etc.;

f) asegurarse de que no se exceda el número máximo de usuarios o recursos [por ejemplo, unidades centrales de procesamiento (CPU)] permitido dentro de la licencia;

g) llevar a cabo revisiones para garantizar que solo se instalen software autorizado y productos con licencia;

h) proporcionar procedimientos para mantener las condiciones apropiadas de la licencia;

i) proporcionar procedimientos para desechar o transferir software a otros;

j) cumplir con los términos y condiciones del software y la información obtenida de redes públicas y fuentes externas;

k) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (video, audio) que no sea lo permitido por la ley de derechos de autor o las licencias aplicables;

l) no copiar, total o parcialmente, normas (p. ej. Normas Internacionales ISO/IEC), libros, artículos, informes u otros documentos, salvo lo permitido por la ley de derechos de autor o las licencias aplicables.

Otra información

Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código fuente.

Los productos de software patentados generalmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando la copia a la creación de copias de seguridad únicamente. Consulte la serie ISO/IEC 19770 para obtener detalles sobre la gestión de activos de TI.

Los datos se pueden obtener de fuentes externas. En general, se da el caso de que dichos datos se obtienen bajo los términos de un acuerdo de intercambio de datos o un instrumento legal similar. Dichos acuerdos de intercambio de datos deben dejar claro qué procesamiento está permitido para los datos adquiridos. También es recomendable que se indique claramente la procedencia de los datos. Ver ISO/IEC 23751: -[1)]para obtener detalles sobre los acuerdos de intercambio de datos.

Los requisitos legales, estatutarios, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado. En particular, pueden exigir que solo se pueda utilizar el material desarrollado por la organización o que el desarrollador haya autorizado o proporcionado a la organización. La infracción de los derechos de autor puede dar lugar a acciones legales, que pueden implicar multas y procesos penales.

Aparte de la necesidad de que la organización cumpla con sus obligaciones con respecto a los derechos de propiedad intelectual de terceros, también deben gestionarse los riesgos del personal y de terceros que no respeten los derechos de propiedad intelectual de la organización.

1) En preparación. Etapa en el momento de la publicación: ISO/IEC PRF 23751:2022.

5.33 Protección de registros

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Legal_y_cumplimiento # Gestión de activos # Information_protec- ción	# Defensa

Control

Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.

Propósito

Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales, así como las expectativas de la comunidad o la sociedad relacionadas con la protección y disponibilidad de los registros.

Guia

La organización debe tomar los siguientes pasos para proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, ya que su contexto comercial y los requisitos para su gestión cambian con el tiempo:

a) emitir lineamientos sobre el almacenamiento, el manejo de la cadena de custodia y la eliminación de registros, lo que incluye la prevención de la manipulación de registros. Estas pautas deben estar alineadas con la política específica del tema de la organización sobre la gestión de registros y otros requisitos de registros;

b) elaborar un calendario de conservación que defina los registros y el período de tiempo durante el cual deben conservarse.

El sistema de almacenamiento y manejo debe garantizar la identificación de los registros y de su período de retención teniendo en cuenta la legislación o los reglamentos nacionales o regionales, así como las expectativas de la comunidad o la sociedad, si corresponde. Este sistema debería permitir la destrucción adecuada de registros después de ese período si la organización no los necesita.

Al decidir sobre la protección de registros organizacionales específicos, se debe considerar su clasificación de seguridad de la información correspondiente, con base en el esquema de clasificación de la organización. Los registros deben clasificarse en tipos de registros (p. ej., registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles sobre los períodos de retención y el tipo de medio de almacenamiento permitido, que puede ser físico o electrónico.

Los sistemas de almacenamiento de datos deben elegirse de manera que los registros requeridos puedan recuperarse en un marco de tiempo y formato aceptables, según los requisitos que se deban cumplir.

Cuando se elijan medios de almacenamiento electrónico, se deben establecer procedimientos para garantizar la capacidad de acceder a los registros (tanto los medios de almacenamiento como la legibilidad del formato) durante todo el período de retención para salvaguardar contra pérdidas debido a futuros cambios tecnológicos. Cualquier clave criptográfica relacionada y programas asociados con archivos cifrados o firmas digitales también deben conservarse para permitir el descifrado de los registros durante el tiempo que se conservan los registros (ver8.24).

Los procedimientos de almacenamiento y manipulación deben implementarse de acuerdo con las recomendaciones proporcionadas por los fabricantes de los medios de almacenamiento. Se debe considerar la posibilidad de deterioro de los medios utilizados para el almacenamiento de registros.

Otra información

Los registros documentan eventos o transacciones individuales o pueden formar agregados que han sido diseñados para documentar procesos de trabajo, actividades o funciones. Ambos son evidencia de actividad comercial y activos de información. Cualquier conjunto de información, independientemente de su estructura o forma, puede gestionarse como un

registro. Esto incluye información en forma de documento, una recopilación de datos u otros tipos de información digital o análoga que se crean, capturan y gestionan en el curso del negocio.

En la gestión de documentos, los metadatos son datos que describen el contexto, el contenido y la estructura de los documentos, así como su gestión a lo largo del tiempo. Los metadatos son un componente esencial de cualquier registro.

Puede ser necesario conservar algunos registros de forma segura para cumplir con los requisitos legales, estatutarios, reglamentarios o contractuales, así como para respaldar las actividades comerciales esenciales. La ley o regulación nacional puede establecer el período de tiempo y el contenido de los datos para la retención de la información. Puede encontrar más información sobre la gestión de registros en la norma ISO 15489.

5.34 Privacidad y protección de PII

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Información_protección # Legal_y_cumplimiento	# Proteccion

Control

La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

Propósito

Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de PII.

Guia

La organización debe establecer y comunicar una política de privacidad y protección de PII específica del tema a todas las partes interesadas pertinentes.

La organización debe desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la PII. Estos procedimientos deben comunicarse a todas las partes interesadas relevantes involucradas en el procesamiento de información de identificación personal.

El cumplimiento de estos procedimientos y de toda la legislación y los reglamentos pertinentes relacionados con la preservación de la privacidad y la protección de la PII requiere roles, responsabilidades y controles apropiados. A menudo, esto se logra mejor mediante el nombramiento de una persona responsable, como un oficial de privacidad, que debe brindar orientación al personal, los proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deben seguirse.

La responsabilidad por el manejo de la PII debe abordarse teniendo en cuenta la legislación y los reglamentos pertinentes.

Se deben implementar medidas técnicas y organizativas apropiadas para proteger la PII.

Otra información

Varios países han introducido legislación que impone controles sobre la recopilación, el procesamiento, la transmisión y la eliminación de PII. Dependiendo de la legislación nacional respectiva, dichos controles pueden imponer obligaciones a quienes recopilan, procesan y difunden PII y también pueden restringir la autoridad para transferir PII a otros países.

ISO/IEC 29100 proporciona un marco de alto nivel para la protección de PII dentro de los sistemas de TIC. Se puede encontrar más información sobre los sistemas de gestión de información de privacidad en ISO / IEC 27701. Se puede encontrar información específica sobre la gestión de información de privacidad para nubes públicas que actúan como procesadores de PII en ISO / IEC 27018.

ISO/IEC 29134 proporciona pautas para la evaluación del impacto en la privacidad (PIA) y proporciona un ejemplo de la estructura y el contenido de un informe PIA. En comparación con ISO/IEC 27005, se centra en el procesamiento de PII y es relevante para aquellas organizaciones que procesan PII. Esto puede ayudar a identificar los riesgos de privacidad y las posibles mitigaciones para reducir estos riesgos a niveles aceptables.

5.35 Revisión independiente de la seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Cor-correctivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Information_security_assurance	# Gobernanza_y_Ecosistema

Control

El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Propósito

Asegurar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.

Guia

La organización debe tener procesos para realizar revisiones independientes.

La gerencia debe planificar e iniciar revisiones periódicas independientes. Las revisiones deben incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad de la información, incluida la política de seguridad de la información, las políticas de temas específicos y otros controles.

Dichas revisiones deben ser realizadas por personas independientes del área bajo revisión (por ejemplo, la función de auditoría interna, un gerente independiente o una organización externa especializada en tales revisiones). Las personas que lleven a cabo estas revisiones deben tener la competencia adecuada. La persona que realiza las revisiones no debe estar en la línea de autoridad para garantizar que tenga la independencia para realizar una evaluación.

Los resultados de las revisiones independientes deben informarse a la dirección que inició las revisiones y, si procede, a la alta dirección. Estos registros deben mantenerse.

Si las revisiones independientes identifican que el enfoque y la implementación de la organización para gestionar la seguridad de la información son inadecuados [por ejemplo, los objetivos y requisitos documentados no se cumplen o no cumplen con la dirección para la seguridad de la información establecida en la política de seguridad de la información y las políticas específicas del tema (ver5.1)], la gerencia debe iniciar acciones correctivas.

Además de las revisiones independientes periódicas, la organización debería considerar la realización de revisiones independientes cuando:

a) leyes y reglamentos que afectan el cambio de la organización;

b) ocurren incidentes significativos;

c) la organización inicia un nuevo negocio o cambia un negocio actual;

d) la organización comienza a usar un nuevo producto o servicio, o cambia el uso de un producto o servicio actual;

e) la organización cambia significativamente los controles y procedimientos de seguridad de la información.

Otra información

ISO/IEC 27007 e ISO/IEC TS 27008 brindan orientación para llevar a cabo revisiones independientes.

5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Capacidad operativa dades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger	# Legal_and_compli-ance # Information_securi-ty_assurance	# Gobernanza_y_ Ecosistema

Control

El cumplimiento de la política de seguridad de la información de la organización, las políticas específicas del tema, las reglas y los estándares debe revisarse periódicamente.

Propósito

Para garantizar que la seguridad de la información se implemente y opere de acuerdo con la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema.

Guia

Los gerentes, propietarios de servicios, productos o información deben identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política de seguridad de la información, las políticas específicas del tema, las reglas, los estándares y otras reglamentaciones aplicables. Se deben considerar herramientas automáticas de medición y generación de informes para una revisión periódica eficiente.

Si se encuentra algún incumplimiento como resultado de la revisión, los gerentes deben:

a) identificar las causas del incumplimiento;

b) evaluar la necesidad de acciones correctivas para lograr el cumplimiento;

c) implementar acciones correctivas apropiadas;

d) revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

Los resultados de las revisiones y acciones correctivas llevadas a cabo por los gerentes, propietarios de servicios, productos o información deben registrarse y estos registros deben mantenerse. Los gerentes deben informar los resultados a las personas que realizan las revisiones independientes (ver5.35) cuando se lleve a cabo una revisión independiente en el área de su responsabilidad.

Las acciones correctivas deben completarse de manera oportuna según corresponda al riesgo. Si no se completa para la próxima revisión programada, el progreso debe al menos abordarse en esa revisión.

Otra información

El monitoreo operativo del uso del sistema está cubierto en8.15 ,8.16 ,8.17 .

5.37 Procedimientos operativos documentados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Recuperar	# Gestión de activos # Seguridad física # sistema_y_red-trabajo_seguridad #Aplicación_seguridad # configuración_segura #Identidad_y_acceso_administración # Threat_and_vulnera-bility_management # Continuidad # Information_securi-ty_event_management	# Gobernanza_y_Ecosistema # Protección ción # Defensa

Control

Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

Propósito

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

Guia

Se deben preparar procedimientos documentados para las actividades operativas de la organización asociadas con la seguridad de la información, por ejemplo:

a) cuando la actividad deba ser realizada de la misma manera por muchas personas;

b) cuando la actividad se realiza con poca frecuencia y cuando se realiza la próxima vez es probable que se haya olvidado el procedimiento;

c) cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente;

d) antes del traspaso de la actividad al nuevo personal.

Los procedimientos operativos deben especificar:

a) las personas responsables;

b) la instalación y configuración segura de sistemas;

c) procesamiento y manejo de información, tanto automatizado como manual;

d) copia de seguridad (ver8.13) y resiliencia;

e) requisitos de programación, incluidas las interdependencias con otros sistemas;

f) instrucciones para el manejo de errores u otras condiciones excepcionales [por ejemplo, restricciones en el uso de programas de utilidad (ver8.18)], que pueden surgir durante la ejecución del trabajo;

g) contactos de soporte y escalamiento, incluidos contactos de soporte externo en caso de dificultades operativas o técnicas inesperadas;

h) instrucciones de manejo de medios de almacenamiento (ver7.10 y7.14);

i) procedimientos de reinicio y recuperación del sistema para su uso en caso de falla del sistema;

j) la gestión de la pista de auditoría y la información de registro del sistema (ver8.15 y8.17) y sistemas de vigilancia por vídeo (ver7.4);

k) procedimientos de seguimiento tales como capacidad, desempeño y seguridad (ver8.6 y8.16);

l) instrucciones de mantenimiento.

Los procedimientos operativos documentados deben revisarse y actualizarse cuando sea necesario. Los cambios a los procedimientos operativos documentados deben ser autorizados. Cuando sea técnicamente factible, los sistemas de información deben administrarse de manera consistente, utilizando los mismos procedimientos, herramientas y utilidades.

Otra información

Ninguna otra información.

6 Controles de personas

6.1 Cribado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

Control

Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y la riesgos percibidos.

Propósito

Asegurar que todo el personal sea elegible y adecuado para las funciones para las que se le considera y siga siendo elegible y adecuado durante su empleo.

Guia

Se debe realizar un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Cuando estas personas sean contratadas a través de proveedores de servicios, los requisitos de selección deben incluirse en los acuerdos contractuales entre la organización y los proveedores.

La información sobre todos los candidatos que se están considerando para puestos dentro de la organización debe recopilarse y manejarse teniendo en cuenta la legislación pertinente que exista en la jurisdicción correspondiente. En algunas jurisdicciones, la organización puede estar legalmente obligada a informar a los candidatos de antemano sobre las actividades de selección.

La verificación debe tener en cuenta toda la legislación relevante sobre privacidad, protección de PII y basada en el empleo y, cuando esté permitido, debe incluir lo siguiente:

a) disponibilidad de referencias satisfactorias (por ejemplo, referencias comerciales y personales);

b) una verificación (de integridad y exactitud) del currículum vitae del solicitante;

c) confirmación de las calificaciones académicas y profesionales reclamadas;

d) verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable emitido por las autoridades correspondientes);

e) verificación más detallada, como revisión de crédito o revisión de antecedentes penales si el candidato asume un papel crítico.

Cuando se contrata a una persona para una función específica de seguridad de la información, la organización debe asegurarse de que el candidato:

a) tiene la competencia necesaria para desempeñar la función de seguridad;

b) se puede confiar para asumir el rol, especialmente si el rol es crítico para la organización.

Cuando un trabajo, ya sea en el nombramiento inicial o en la promoción, implique que la persona tenga acceso a instalaciones de procesamiento de información y, en particular, si esto implica el manejo de información confidencial (por ejemplo, información financiera, información personal o información de atención médica), la organización también debe considerar más , verificaciones más detalladas.

Los procedimientos deben definir los criterios y limitaciones para las revisiones de verificación (por ejemplo, quién es elegible para evaluar a las personas y cómo, cuándo y por qué se llevan a cabo las revisiones de verificación).

En situaciones en las que la verificación no se puede completar de manera oportuna, se deben implementar controles de mitigación hasta que se haya terminado la revisión, por ejemplo:

a) incorporación retrasada;

b) retraso en el despliegue de los activos corporativos;

c) embarque con acceso reducido;

d) terminación del empleo.

Los controles de verificación deben repetirse periódicamente para confirmar la idoneidad continua del personal, según la importancia del rol de una persona.

Otra información

Ninguna otra información.

6.2 Términos y condiciones de empleo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

Control

Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

Propósito

Asegurar que el personal comprenda sus responsabilidades de seguridad de la información para las funciones para las que se le considera.

Guia

Las obligaciones contractuales para el personal deben tener en cuenta la política de seguridad de la información de la organización y las políticas específicas del tema relevante. Además, se pueden aclarar y señalar los siguientes puntos:

a) acuerdos de confidencialidad o de no divulgación que el personal al que se le da acceso a información confidencial debe firmar antes de que se le dé acceso a la información y otros activos asociados (ver 6.6);

b) responsabilidades y derechos legales [por ejemplo, con respecto a las leyes de derechos de autor o la legislación de protección de datos (ver 5.32 y5.34)];

c) responsabilidades para la clasificación de la información y la gestión de la información de la organización y otros activos asociados, instalaciones de procesamiento de información y servicios de información manejados por el personal (ver5.9 para5.13);

d) responsabilidades por el tratamiento de la información recibida de los interesados;

e) acciones a tomar si el personal ignora los requisitos de seguridad de la organización (ver6.4).

Las funciones y responsabilidades de seguridad de la información deben comunicarse a los candidatos durante el proceso previo al empleo.

La organización debe asegurarse de que el personal esté de acuerdo con los términos y condiciones relacionados con la seguridad de la información. Estos términos y condiciones deben ser apropiados para la naturaleza y el grado de acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información. Los términos y condiciones relacionados con la seguridad de la información deben revisarse cuando cambien las leyes, los reglamentos, la política de seguridad de la información o las políticas específicas de un tema.

En su caso, las responsabilidades contenidas en los términos y condiciones de empleo deben continuar durante un período definido después de la terminación del empleo (ver6.5).

Otra información

Se puede utilizar un código de conducta para establecer las responsabilidades de seguridad de la información del personal con respecto a la confidencialidad, la protección de la PII, la ética, el uso apropiado de la información de la organización y otros activos asociados, así como las prácticas respetables esperadas por la organización.

Es posible que se requiera que una parte externa, con la que está asociado el personal del proveedor, celebre acuerdos contractuales en nombre de la persona contratada.

Si la organización no es una entidad legal y no tiene empleados, se puede considerar el equivalente de un acuerdo contractual y términos y condiciones de acuerdo con la orientación de este control.

6.3 Concientización, educación y capacitación en seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad	# Gobernanza_y_ Ecosistema

Control

El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.

Propósito

Asegurar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades de seguridad de la información.

Guia

General

Se debe establecer un programa de concientización, educación y capacitación en seguridad de la información de acuerdo con la política de seguridad de la información de la organización, las políticas específicas del tema y los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la organización que debe protegerse y los controles de seguridad de la información que se han implementado. para proteger la información.

La concientización, la educación y la capacitación en seguridad de la información deben llevarse a cabo periódicamente. La concientización, la educación y la capacitación iniciales pueden aplicarse al personal nuevo y a aquellos que se transfieran a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes.

La comprensión del personal debe evaluarse al final de una actividad de concientización, educación o capacitación para probar la transferencia de conocimientos y la efectividad del programa de concientización, educación y capacitación.

Conciencia

Un programa de concientización sobre la seguridad de la información debe tener como objetivo que el personal sea consciente de sus responsabilidades con respecto a la seguridad de la información y los medios por los cuales se cumplen esas responsabilidades.

El programa de sensibilización debe planificarse teniendo en cuenta las funciones del personal de la organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal del proveedor). Las actividades del programa de concientización deben programarse a lo largo del tiempo, preferiblemente con regularidad, para que las actividades se repitan y cubran al personal nuevo. También debe basarse en las lecciones aprendidas de los incidentes de seguridad de la información.

El programa de sensibilización debe incluir una serie de actividades de sensibilización a través de canales físicos o virtuales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, sesiones informativas, módulos de aprendizaje electrónico y correos electrónicos.

La concientización sobre la seguridad de la información debe cubrir aspectos generales tales como:

a) el compromiso de la dirección con la seguridad de la información en toda la organización;

b) las necesidades de familiarización y cumplimiento con respecto a las reglas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, normas, leyes, estatutos, reglamentos, contratos y acuerdos específicos del tema;

c) responsabilidad personal por las propias acciones e inacciones, y responsabilidades generales para asegurar o proteger la información que pertenece a la organización y las partes interesadas;

d) procedimientos básicos de seguridad de la información [por ejemplo, informes de eventos de seguridad de la información (6.8)] y controles básicos [por ejemplo, seguridad de contraseña (5.17)];

e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre asuntos de seguridad de la información, incluidos más materiales de concientización sobre la seguridad de la información.

Educación y entrenamiento

La organización debe identificar, preparar e implementar un plan de capacitación adecuado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y experiencia específicos. Los equipos técnicos deben tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios. Si faltan habilidades, la organización debe tomar medidas y adquirirlas.

El programa de educación y capacitación debe considerar diferentes formas [por ejemplo, conferencias o autoaprendizaje, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutar personas ya capacitadas y contratar consultores]. Puede usar diferentes medios de entrega, incluidos el aprendizaje en el aula, a distancia, basado en la web, a su propio ritmo y otros. El personal técnico debe mantener actualizados sus conocimientos suscribiéndose a boletines y revistas o asistiendo a congresos y eventos destinados a la mejora técnica y profesional.

Otra información

Al redactar un programa de concientización, es importante no solo centrarse en el 'qué' y el 'cómo', sino también en el 'por qué', cuando sea posible. Es importante que el personal comprenda el objetivo de la seguridad de la información y el efecto potencial, positivo y negativo, sobre la organización de su propio comportamiento.

La concientización, la educación y la capacitación en seguridad de la información pueden ser parte de, o llevarse a cabo en colaboración con otras actividades, por ejemplo, administración general de la información, TIC, seguridad, privacidad o capacitación en seguridad.

6.4 Proceso disciplinario

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Cor-correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Responder	# Recursos humanos_seguridad	# Gobernanza_y_Ecosistema

Control

Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

Propósito

Asegurar que el personal y otras partes interesadas relevantes entiendan las consecuencias de la violación de la política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas relevantes que cometieron la violación.

Guia

El proceso disciplinario no debe iniciarse sin la verificación previa de que se ha producido una violación de la política de seguridad de la información (ver5.28).

El proceso disciplinario formal debe prever una respuesta graduada que tenga en cuenta factores tales como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad del incumplimiento y sus consecuencias;

b) si el delito fue intencional (malicioso) o no intencional (accidental);

c) si se trata o no de una primera o reiterada infracción;

d) si el infractor fue debidamente capacitado o no.

La respuesta debe tener en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales y comerciales pertinentes, así como otros factores que sean necesarios. El proceso disciplinario también debe utilizarse como elemento disuasorio para evitar que el personal y otras partes interesadas pertinentes violen la política de seguridad de la información, las políticas y los procedimientos específicos del tema para la seguridad de la información. Las violaciones deliberadas de la política de seguridad de la información pueden requerir acciones inmediatas.

Otra información

Siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias debe protegerse de conformidad con los requisitos aplicables.

Cuando las personas demuestran un comportamiento excelente con respecto a la seguridad de la información, pueden ser recompensadas para promover la seguridad de la información y fomentar el buen comportamiento.

6.5 Responsabilidades después de la terminación o cambio de empleo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Recursos humanos_ seguridad # Gestión de activos	# Gobernanza_y_ Ecosistema

Control

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deben definirse, aplicarse y comunicarse al personal pertinente y otras partes interesadas.

Propósito

Para proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos.

Guia

El proceso para gestionar la terminación o el cambio de empleo debe definir qué responsabilidades y deberes de seguridad de la información deben permanecer vigentes después de la terminación o el cambio. Esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (ver6.6). Las responsabilidades y deberes que sigan siendo válidos después de la terminación del empleo o del contrato deben figurar en los términos y condiciones de empleo de la persona (ver6.2), contrato o acuerdo. Otros contratos o acuerdos que continúan por un período definido después del final del empleo del individuo también pueden contener responsabilidades de seguridad de la información.

Los cambios de responsabilidad o empleo deben gestionarse como la terminación de la responsabilidad o empleo actual combinada con el inicio de la nueva responsabilidad o empleo.

Las funciones y responsabilidades de seguridad de la información que tenga cualquier persona que deje o cambie de puesto deben identificarse y transferirse a otra persona.

Debe establecerse un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, otras partes interesadas y personas de contacto pertinentes (por ejemplo, clientes y proveedores).

El proceso de terminación o cambio de empleo también debe aplicarse al personal externo (es decir, proveedores) cuando se produzca una terminación del personal, del contrato o del puesto con la organización, o cuando haya un cambio de puesto dentro de la organización.

Otra información

En muchas organizaciones, la función de recursos humanos generalmente es responsable del proceso general de terminación y trabaja junto con el gerente supervisor de la persona en transición para administrar los aspectos de seguridad de la información de los procedimientos relevantes. En el caso de personal proporcionado a través de una parte externa (por ejemplo, a través de un proveedor), este proceso de terminación lo lleva a cabo la parte externa de acuerdo con el contrato entre la organización y la parte externa.

6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Recursos_humanos_seguridad # Información_protección # relaciones_con_proveedores	# Gobernanza_y_ Ecosistema

Control

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

Propósito

Para mantener la confidencialidad de la información accesible por el personal o partes externas.

Guia

Los acuerdos de confidencialidad o de no divulgación deben abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Con base en los requisitos de seguridad de la información de una organización, los términos de los acuerdos deben determinarse tomando en consideración el tipo de información que se manejará, su nivel de clasificación, su uso y el acceso permitido por la otra parte. Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se deben considerar los siguientes elementos:

a) una definición de la información a proteger (por ejemplo, información confidencial);

b) la duración esperada de un acuerdo, incluidos los casos en los que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente;

c) las acciones requeridas cuando se termina un acuerdo;

d) las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada;

e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;

f) el uso permitido de la información confidencial y los derechos del firmante para usar la información;

g) el derecho a auditar y monitorear actividades que involucren información confidencial para circunstancias altamente sensibles;

h) el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial;

i) los términos para la devolución o destrucción de la información al término del contrato;

j) las acciones previstas a tomar en caso de incumplimiento del acuerdo.

La organización debe tener en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación para la jurisdicción a la que se aplican (ver5.31 ,5.32 ,5.33 ,5.34).

Los requisitos para los acuerdos de confidencialidad y no divulgación deben revisarse periódicamente y cuando ocurran cambios que influyan en estos requisitos.

Otra información

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada.

6.7 Trabajo a distancia

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gestión de activos # Information_protec-ción # Seguridad física # sistema_y_red-trabajo_seguridad	# Proteccion

Control

Se deben implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.

Propósito

Para garantizar la seguridad de la información cuando el personal está trabajando de forma remota.

Guia

El trabajo remoto ocurre cuando el personal de la organización trabaja desde una ubicación fuera de las instalaciones de la organización, accediendo a la información ya sea en forma impresa o electrónica a través de equipos de TIC. Los entornos de trabajo remoto incluyen los denominados "teletrabajo", "teletrabajo", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "mantenimiento remoto".

NOTA Es posible que no todas las recomendaciones de esta guía se puedan aplicar debido a la legislación local. y regulaciones en diferentes jurisdicciones.

Las organizaciones que permiten actividades de trabajo a distancia deben emitir una política específica sobre el tema del trabajo a distancia que defina las condiciones y restricciones pertinentes. Cuando se considere aplicable, se deben considerar los siguientes asuntos:

a) la seguridad física existente o propuesta del sitio de trabajo remoto, teniendo en cuenta la seguridad física del lugar y el entorno local, incluidas las diferentes jurisdicciones donde se encuentra el personal;

b) reglas y mecanismos de seguridad para el entorno físico remoto, como archivadores con cerradura, transporte seguro entre ubicaciones y reglas para el acceso remoto, escritorio despejado, impresión y eliminación de información y otros activos asociados, e informes de eventos de seguridad de la información (ver6.8);

c) los entornos físicos de trabajo remoto esperados;

d) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la organización, la sensibilidad de la información a la que se accederá y pasará por el enlace de comunicación y la sensibilidad de los sistemas y aplicaciones;

e) el uso de acceso remoto, como acceso de escritorio virtual que admita el procesamiento y almacenamiento de información en equipos de propiedad privada;

f) la amenaza de acceso no autorizado a información o recursos de otras personas en el lugar de trabajo remoto (por ejemplo, familiares y amigos);

g) la amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos;

h) el uso de redes domiciliarias y redes públicas, y requisitos o restricciones en la configuración de servicios de redes inalámbricas;

i) uso de medidas de seguridad, como firewalls y protección contra malware;

j) mecanismos seguros para implementar e inicializar sistemas de forma remota;

k) mecanismos seguros de autenticación y habilitación de privilegios de acceso teniendo en cuenta la vulnerabilidad de los mecanismos de autenticación de un solo factor donde se permite el acceso remoto a la red de la organización.

Las directrices y medidas a considerar deben incluir:

a) la provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo remoto, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;

b) una definición del trabajo permitido, la clasificación de la información que puede ser mantenida y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder;

c) la provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo. Esto debe incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota;

d) la provisión de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto, como los requisitos sobre bloqueos de pantalla del dispositivo y temporizadores de inactividad; la habilitación del seguimiento de la ubicación del dispositivo; instalación de capacidades de borrado remoto;

e) seguridad física;

f) reglas y orientación sobre el acceso de familiares y visitantes a equipos e información;

g) la provisión de soporte y mantenimiento de hardware y software;

h) la provisión de seguros;

i) los procedimientos de respaldo y continuidad del negocio;

j) auditoría y seguimiento de la seguridad;

k) revocación de facultades y derechos de acceso y devolución de equipos cuando finalicen las actividades de trabajo a distancia.

Otra información

Ninguna otra información.

6.8 Reporte de eventos de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective	# Confidencialidad # Integridad # Disponibilidad	# Detectar	# Information_security_event_management	# Defensa

Control

La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

Propósito

Para respaldar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que pueden ser identificados por el personal.

Guia

Todo el personal y los usuarios deben ser conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.

También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se deben informar los eventos. El mecanismo de presentación de informes debe ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades.

Las situaciones a considerar para el reporte de eventos de seguridad de la información incluyen:

a) controles de seguridad de la información ineficaces;

b) incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;

c) errores humanos;

d) incumplimiento de la política de seguridad de la información, políticas específicas del tema o normas aplicables;

e) incumplimientos de las medidas de seguridad física;

f) cambios del sistema que no han pasado por el proceso de gestión de cambios;

g) mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware;

h) infracciones de acceso;

i) vulnerabilidades;

j) sospecha de infección por malware.

Se debe advertir al personal y a los usuarios que no intenten probar vulnerabilidades de seguridad de la información sospechosas. Las vulnerabilidades de prueba pueden interpretarse como un mal uso potencial del sistema y también pueden causar daños al sistema o servicio de información, y pueden corromper u ocultar la evidencia digital. En última instancia, esto puede resultar en responsabilidad legal para la persona que realiza la prueba.

Otra información

Consulte la serie ISO/IEC 27035 para obtener información adicional.

7 controles físicos

7.1 Perímetros de seguridad física

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física	# Proteccion

Control

Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

Propósito

Para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.

Guia

Las siguientes pautas deben considerarse e implementarse cuando corresponda para los perímetros de seguridad física:

a) definir los perímetros de seguridad y la ubicación y fortaleza de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro;

b) tener perímetros físicamente sólidos para un edificio o sitio que contenga instalaciones de procesamiento de información (es decir, no debe haber espacios en el perímetro o áreas donde pueda ocurrir fácilmente un allanamiento).
Los techos, paredes, techos y pisos exteriores del sitio deben ser de construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, rejas, alarmas, cerraduras). Las puertas y ventanas deben cerrarse con llave cuando estén desatendidas y se debe considerar la protección externa para las ventanas, particularmente a nivel del suelo; también se deben considerar los puntos de ventilación;

c) alarmar, monitorear y probar todas las puertas contra incendios en un perímetro de seguridad junto con las paredes para establecer el nivel requerido de resistencia de acuerdo con los estándares adecuados. Deben operar de manera a prueba de fallas.

Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de las instalaciones de la organización y las instalaciones de procesamiento de información.

Un área segura puede ser una oficina con cerradura o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Es posible que se necesiten barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. La organización debe considerar tener medidas de seguridad física que puedan fortalecerse durante situaciones de mayor amenaza.

7.2 Entrada física

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Identity_and_Access_Management	# Proteccion

Control

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.

Propósito

Para garantizar que solo se produzca el acceso físico autorizado a la información de la organización y otros activos asociados.

Guia

General

Los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Se deben considerar las siguientes pautas:

a) restringir el acceso a los sitios y edificios solo al personal autorizado. El proceso de gestión de los derechos de acceso a las áreas físicas debe incluir el otorgamiento, revisión periódica, actualización y revocación de las autorizaciones (ver5.18);

b) mantener y monitorear de forma segura un libro de registro físico o un registro de auditoría electrónico de todos los accesos y proteger todos los registros (ver5.33) e información confidencial de autenticación;

c) establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Se deben considerar puertas dobles de seguridad para el acceso a áreas sensibles;

d) establecer un área de recepción monitoreada por personal u otros medios para controlar el acceso físico al sitio o edificio;

e) inspeccionar y examinar los efectos personales del personal y de los interesados a la entrada y salida;

NOTA Puede existir legislación y reglamentos locales con respecto a la posibilidad de inspeccionar pertenencias.

f) exigir que todo el personal y las partes interesadas usen algún tipo de identificación visible y que notifiquen de inmediato al personal de seguridad si encuentran visitantes sin escolta y cualquier persona que no use una identificación visible. Se deben considerar insignias fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes;

g) otorgar acceso restringido al personal del proveedor a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso debe ser autorizado y monitoreado;

h) prestar especial atención a la seguridad del acceso físico en el caso de edificios que contengan activos para múltiples organizaciones;

i) diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos;

j) proteger otros puntos de entrada, como salidas de emergencia, del acceso no autorizado;

k) establecer un proceso de gestión de claves para garantizar la gestión de las claves físicas o la información de autenticación (p. ej., códigos de bloqueo, cerraduras de combinación para oficinas, salas e instalaciones, como armarios de llaves) y garantizar un libro de registro o una auditoría anual de claves y que el acceso a claves físicas o se controla la información de autenticación (ver5.17 para obtener más orientación sobre la información de autenticación).

Visitantes

Se deben considerar las siguientes pautas:

a) autenticar la identidad de los visitantes por un medio apropiado;

b) registrar la fecha y hora de entrada y salida de los visitantes;

c) permitir el acceso de visitantes únicamente para fines específicos, autorizados y con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia;

d) supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

Zonas de entrega y carga y entrada de material

Se deben considerar las siguientes pautas:

a) restringir el acceso a las áreas de entrega y carga desde el exterior del edificio al personal identificado y autorizado;

b) diseñar las áreas de entrega y carga para que las entregas puedan cargarse y descargarse sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio;

c) asegurar las puertas externas de las áreas de entrega y carga cuando se abren las puertas de las áreas restringidas;

d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que se muevan de las áreas de entrega y carga;

e) registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos (ver5.9 y 7.10) al ingresar al sitio;

f) separar físicamente los envíos entrantes y salientes, cuando sea posible;

g) inspeccionar las entregas entrantes en busca de evidencia de manipulación en la carretera. Si se descubre una manipulación, se debe informar de inmediato al personal de seguridad.

Otra información

Ninguna otra información.

7.3 Aseguramiento de oficinas, salas e instalaciones

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion

Control

Debe diseñarse e implementarse la seguridad física de las oficinas, salas e instalaciones.

Propósito

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.

Guia

Se deben considerar las siguientes pautas para asegurar oficinas, salas e instalaciones:

a) ubicar las instalaciones críticas para evitar el acceso del público;

b) cuando corresponda, asegurarse de que los edificios sean discretos y den una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, que identifiquen la presencia de actividades de procesamiento de información;

c) configurar instalaciones para evitar que la información o actividades confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también debe considerarse apropiado;

d) no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen las ubicaciones de las instalaciones de procesamiento de información confidencial.

Otra información

Ninguna otra información.

7.4 Supervisión de la seguridad física

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# Seguridad física	# Proteccion # Defensa

Control

Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

Propósito

Para detectar y disuadir el acceso físico no autorizado.

Guia

Las instalaciones físicas deben ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de monitoreo de video como un circuito cerrado de televisión y software de gestión de información de seguridad física, ya sea administrado internamente o por un proveedor de servicios de monitoreo.

El acceso a los edificios que albergan sistemas críticos debe monitorearse continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante:

a) instalar sistemas de vigilancia por video, como un circuito cerrado de televisión, para ver y registrar el acceso a áreas sensibles dentro y fuera de las instalaciones de una organización;

b) instalar, de acuerdo con las normas pertinentes aplicables, y probar periódicamente detectores de contacto, sonido o movimiento para activar una alarma de intrusión, tales como:

1) instalar detectores de contacto que activen una alarma cuando se haga o se rompa un contacto en cualquier lugar donde se pueda hacer o romper un contacto (como ventanas y puertas y debajo de objetos) para ser utilizado como alarma de pánico;

2) detectores de movimiento basados en tecnología infrarroja que activan una alarma cuando un objeto pasa por su campo de visión;

3) instalar sensores sensibles al sonido de cristales rotos que puedan usarse para activar una alarma para alertar al personal de seguridad;

c) usar esas alarmas para cubrir todas las puertas exteriores y ventanas accesibles. Las áreas desocupadas deben estar alarmadas en todo momento; también se debe proporcionar cobertura para otras áreas (por ejemplo, salas de computadoras o de comunicaciones).

El diseño de los sistemas de monitoreo debe mantenerse confidencial porque la divulgación puede facilitar robos no detectados.

Los sistemas de monitoreo deben protegerse contra el acceso no autorizado para evitar que personas no autorizadas accedan a la información de vigilancia, como transmisiones de video, o que los sistemas se deshabiliten de forma remota.

El panel de control del sistema de alarma debe colocarse en una zona de alarma y, para las alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que activa la alarma. El panel de control y los detectores deben tener mecanismos a prueba de manipulaciones. El sistema debe probarse periódicamente para asegurarse de que funciona según lo previsto, especialmente si sus componentes funcionan con baterías.

Cualquier mecanismo de monitoreo y grabación debe usarse teniendo en cuenta las leyes y regulaciones locales, incluida la legislación de protección de datos y PII, especialmente con respecto al monitoreo del personal y los períodos de retención de videos grabados.

Otra información

Ninguna otra información.

7.5 Protección contra amenazas físicas y ambientales

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física	# Proteccion

Control

Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

Propósito

Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.

Guia

Las evaluaciones de riesgos para identificar las posibles consecuencias de las amenazas físicas y ambientales deben realizarse antes de comenzar las operaciones críticas en un sitio físico y en intervalos regulares. Se deben implementar las salvaguardas necesarias y se deben monitorear los cambios en las amenazas. Debe obtenerse asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

La ubicación y la construcción de las instalaciones físicas deben tener en cuenta:

a) topografía local, como elevación adecuada, masas de agua y fallas tectónicas;

b) amenazas urbanas, como lugares con un alto perfil para atraer disturbios políticos, actividad criminal o ataques terroristas.

Con base en los resultados de la evaluación de riesgos, se deben identificar las amenazas físicas y ambientales relevantes y se deben considerar los controles apropiados en los siguientes contextos como ejemplos:

a) incendio: instalar y configurar sistemas capaces de detectar incendios en una etapa temprana para enviar alarmas o activar sistemas de supresión de incendios para evitar que el fuego dañe los medios de almacenamiento y los sistemas de procesamiento de información relacionados. La supresión de incendios debe realizarse utilizando la sustancia más apropiada en relación con el entorno circundante (por ejemplo, gas en espacios confinados);

b) inundaciones: instalar sistemas capaces de detectar inundaciones en una etapa temprana debajo de los pisos de áreas que contienen medios de almacenamiento o sistemas de procesamiento de información. Las bombas de agua o medios equivalentes deberían estar fácilmente disponibles en caso de que ocurra una inundación;

c) sobretensiones eléctricas: adoptar sistemas capaces de proteger los sistemas de información del servidor y del cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos;

d) explosivos y armas: realizar inspecciones aleatorias para detectar la presencia de explosivos o armas en el personal, vehículos o bienes que ingresan a las instalaciones de procesamiento de información sensible.

Otra información

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguras pueden proteger la información almacenada en ellas contra desastres como incendios, terremotos, inundaciones o explosiones.

Las organizaciones pueden considerar los conceptos de prevención del delito a través del diseño ambiental al diseñar los controles para asegurar su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar bolardos, las estatuas o los elementos de agua pueden servir como elemento y barrera física.

7.6 Trabajar en áreas seguras

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física	# Proteccion

Control

Se deben diseñar e implementar medidas de seguridad para trabajar en áreas seguras.

Propósito

Para proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Guia

Las medidas de seguridad para trabajar en áreas seguras deben aplicarse a todo el personal y cubrir todas las actividades que se desarrollen en el área segura.

Se deben considerar las siguientes pautas:

a) hacer que el personal sea consciente de la existencia o de las actividades dentro de un área segura solo según sea necesario;

b) evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas;

c) cerrar físicamente e inspeccionar periódicamente las áreas seguras vacantes;

d) no permitir equipos fotográficos, de video, de audio u otros equipos de grabación, como cámaras en los dispositivos terminales de los usuarios, a menos que estén autorizados;

e) controlar adecuadamente el transporte y uso de los dispositivos de punto final del usuario en áreas seguras;

f) publicar los procedimientos de emergencia de manera fácilmente visible o accesible.

Otra información

Ninguna otra información.

7.7 Escritorio despejado y pantalla despejada

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Seguridad física	# Proteccion

Control

Deben definirse y aplicarse adecuadamente reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de procesamiento de información.

Propósito

Reducir los riesgos de acceso no autorizado, pérdida y daño de la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo.

Guia

La organización debe establecer y comunicar una política específica del tema sobre escritorio despejado y pantalla despejada a todas las partes interesadas relevantes.

Se deben considerar las siguientes pautas:

a) guardar bajo llave la información comercial confidencial o crítica (por ejemplo, en papel o en medios de almacenamiento electrónicos) (idealmente en una caja fuerte, gabinete u otro tipo de mueble de seguridad) cuando no sea necesario, especialmente cuando la oficina esté desocupada;

b) proteger los dispositivos de punto final del usuario mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o desatendidos;

c) dejar los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todas las computadoras y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático;

d) hacer que el originador recopile los resultados de las impresoras o dispositivos multifunción de inmediato. El uso de impresoras con una función de autenticación, de modo que los creadores sean los únicos que puedan obtener sus impresiones y solo cuando estén parados al lado de la impresora;

e) almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial y, cuando ya no se necesiten, desecharlos utilizando mecanismos seguros de eliminación;

f) establecer y comunicar reglas y orientación para la configuración de ventanas emergentes en las pantallas (p. ej., desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública);

g) borrar información sensible o crítica en pizarras y otros tipos de pantallas cuando ya no se necesiten.

La organización debe tener procedimientos implementados al desocupar las instalaciones, incluida la realización de un barrido final antes de irse para garantizar que los activos de la organización no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles).

Otra información

Ninguna otra información.

7.8 Ubicación y protección del equipo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion

Control

El equipo debe estar ubicado de forma segura y protegida.

Propósito

Reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados.

Guia

Se deben considerar las siguientes pautas para proteger el equipo:

a) ubicar el equipo para minimizar el acceso innecesario a las áreas de trabajo y evitar el acceso no autorizado;

b) ubicar cuidadosamente las instalaciones de procesamiento de información que manejan datos confidenciales para reducir el riesgo de que personas no autorizadas vean la información durante su uso;

c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales [por ejemplo, robo, incendio, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo];

d) establecer pautas para comer, beber y fumar en las proximidades de las instalaciones de procesamiento de información;

e) monitorear las condiciones ambientales, como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente la operación de las instalaciones de procesamiento de información;

f) aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las líneas eléctricas y de comunicaciones entrantes;

g) considerar el uso de métodos de protección especiales, como membranas de teclado, para equipos en ambientes industriales;

h) proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética;

i) separar físicamente las instalaciones de procesamiento de información gestionadas por la organización de aquellas que no son gestionadas por la organización.

Otra información

Ninguna otra información.

7.9 Seguridad de los activos fuera de las instalaciones

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion

Control

Los activos fuera del sitio deben estar protegidos.

Propósito

Para evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.

Guia

Cualquier dispositivo utilizado fuera de las instalaciones de la organización que almacene o procese información (p. ej., dispositivo móvil), incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad privada y utilizados en nombre de la organización [traiga su propio dispositivo (BYOD)] necesita protección. El uso de estos dispositivos debe ser autorizado por la gerencia.

Se deben considerar las siguientes pautas para la protección de dispositivos que almacenan o procesan información fuera de las instalaciones de la organización:

a) no dejar desatendidos equipos y medios de almacenamiento fuera de las instalaciones en lugares públicos y no seguros;

b) observar las instrucciones de los fabricantes para proteger el equipo en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo);

c) cuando se transfiere equipo fuera de las instalaciones entre diferentes personas o partes interesadas, mantener un registro que defina la cadena de custodia del equipo que incluya al menos los nombres y organizaciones de quienes son responsables del equipo. La información que no necesita transferirse con el activo debe eliminarse de forma segura antes de la transferencia;

d) cuando sea necesario y práctico, exigir la autorización para retirar equipos y medios de las instalaciones de la organización y mantener un registro de tales retiros para mantener un registro de auditoría (ver5.14);

e) protección contra la visualización de información en un dispositivo (p. ej., móvil o portátil) en el transporte público, y los riesgos asociados con la navegación por el hombro;

f) implementar el seguimiento de la ubicación y la capacidad para el borrado remoto de dispositivos.

La instalación permanente de equipos fuera de las instalaciones de la organización [como antenas y cajeros automáticos (ATM)] puede estar sujeta a un mayor riesgo de daño, robo o escuchas ilegales. Estos riesgos pueden variar considerablemente entre ubicaciones y deben tenerse en cuenta al determinar las medidas más apropiadas. Se deben considerar las siguientes pautas al ubicar este equipo fuera de las instalaciones de la organización:

a) vigilancia de la seguridad física (véase7.4);

b) protección contra amenazas físicas y ambientales (ver7.5);

c) controles de acceso físico ya prueba de manipulaciones;

d) controles de acceso lógico.

Otra información

Puede encontrar más información sobre otros aspectos de la protección de equipos de almacenamiento y procesamiento de información y dispositivos de punto final de usuario en8.1 y6.7 .

7.10 Medios de almacenamiento

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion

Control

Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

Propósito

Garantizar únicamente la divulgación, modificación, eliminación o destrucción autorizada de la información en los medios de almacenamiento.

Guia

Medios de almacenamiento extraíbles

Se deben considerar las siguientes pautas para la gestión de medios de almacenamiento extraíbles:

a) establecer una política específica de un tema sobre la gestión de medios de almacenamiento extraíbles y comunicar dicha política específica de un tema a cualquier persona que use o manipule medios de almacenamiento extraíbles;

b) cuando sea necesario y práctico, solicitar autorización para que los medios de almacenamiento se retiren de la organización y mantener un registro de tales retiros para mantener un registro de auditoría;

c) almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes;

d) si la confidencialidad o la integridad de la información son consideraciones importantes, usar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles;

e) mitigar el riesgo de que los medios de almacenamiento se degraden mientras aún se necesita la información almacenada, transfiriendo la información a nuevos medios de almacenamiento antes de que se vuelva ilegible;

f) almacenar múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información coincidente;

g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) solo habilitar puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas Secure Digital (SD) y puertos de bus serie universal (USB)] si existe una razón organizativa para su uso;

i) cuando sea necesario utilizar medios de almacenamiento extraíbles, monitorear la transferencia de información a dichos medios de almacenamiento;

j) la información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo, cuando se envían medios de almacenamiento a través del servicio postal o de mensajería.

En este control, los medios incluyen documentos en papel. Al transferir medios físicos de almacenamiento, aplique medidas de seguridad en5.14 .

Reutilización o eliminación segura

Deben establecerse procedimientos para la reutilización o eliminación segura de los medios de almacenamiento para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de medios de almacenamiento que contengan información confidencial deben ser proporcionales a la sensibilidad de esa información. Se deben considerar los siguientes elementos:

a) si los medios de almacenamiento que contienen información confidencial deben reutilizarse dentro de la organización, eliminar datos de forma segura o formatear los medios de almacenamiento antes de su reutilización (ver8.10);

b) deshacerse de medios de almacenamiento que contengan información confidencial de forma segura cuando ya no se necesiten (p. ej., destruyendo, triturando o eliminando de forma segura el contenido);

c) contar con procedimientos para identificar los elementos que pueden requerir una eliminación segura;

d) muchas organizaciones ofrecen servicios de recogida y eliminación de medios de almacenamiento. Se debe tener cuidado al seleccionar un proveedor externo adecuado con controles y experiencia adecuados;

e) registrar la eliminación de elementos sensibles para mantener un registro de auditoría;

f) al acumular medios de almacenamiento para su eliminación, teniendo en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no confidencial se convierta en confidencial.

Se debe realizar una evaluación de riesgos en los dispositivos dañados que contienen datos confidenciales para determinar si los elementos deben destruirse físicamente en lugar de enviarse a reparar o desecharse (ver7.14).

Otra información

Cuando la información confidencial en los medios de almacenamiento no está encriptada, se debe considerar la protección física adicional de los medios de almacenamiento.

7.11 Utilidades de apoyo

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Integridad # Disponibilidad	# Proteger #Detectar	# Seguridad física	# Proteccion

Control

Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

Propósito

Para evitar la pérdida, el daño o el compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.

Guia

Las organizaciones dependen de los servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para respaldar sus instalaciones de procesamiento de información. Por lo tanto, la organización debe:

a) asegurarse de que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente;

b) asegurar que las empresas de servicios públicos sean evaluadas regularmente por su capacidad para cumplir con el crecimiento del negocio y las interacciones con otras empresas de servicios públicos de apoyo;

c) asegurarse de que el equipo de apoyo a los servicios públicos sea inspeccionado y probado periódicamente para garantizar su correcto funcionamiento;

d) si es necesario, activar alarmas para detectar fallas en los servicios públicos;

e) si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples alimentaciones con diversas rutas físicas;

f) asegurarse de que el equipo de apoyo a los servicios públicos esté en una red separada de las instalaciones de procesamiento de información si está conectado a una red;

g) asegurarse de que el equipo que respalda a los servicios públicos esté conectado a Internet solo cuando sea necesario y solo de manera segura.

Se debe proporcionar iluminación de emergencia y comunicaciones. Los interruptores y válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios públicos deben ubicarse cerca de las salidas de emergencia o las salas de equipos. Los detalles de los contactos de emergencia deben registrarse y estar disponibles para el personal en caso de un apagón.

Otra información

Se puede obtener redundancia adicional para la conectividad de la red mediante múltiples rutas de más de un proveedor de servicios públicos.

7.12 Seguridad del cableado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Disponibilidad	# Proteger	# Seguridad física	# Proteccion

Control

Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra intercepciones, interferencias o daños.

Propósito

Para evitar la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Guia

Se deben considerar las siguientes pautas para la seguridad del cableado:

a) las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como protectores de cables en el piso y postes de servicios públicos; si los cables son subterráneos, protegerlos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);

b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;

c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:

1) instalación de conductos blindados y cuartos o cajas cerradas y alarmas en los puntos de inspección y terminación;

2) uso de blindaje electromagnético para proteger los cables;

3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;

4) acceso controlado a paneles de conexión y salas de cables (por ejemplo, con llaves mecánicas o PIN);

5) uso de cables de fibra óptica;

d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

Se debe buscar el asesoramiento de especialistas sobre cómo gestionar los riesgos derivados de incidentes o mal funcionamiento del cableado.

Otra información

A veces, el cableado de energía y telecomunicaciones son recursos compartidos por más de una organización que ocupa locales compartidos.

7.13 Mantenimiento de equipos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion # Resiliencia

Control

El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Propósito

Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

Guia

Se deben considerar las siguientes pautas para el mantenimiento del equipo:

a) mantener el equipo de acuerdo con la frecuencia y las especificaciones de servicio recomendadas por el proveedor;

b) implementación y seguimiento de un programa de mantenimiento por parte de la organización;

c) solo personal de mantenimiento autorizado que realice reparaciones y mantenimiento en el equipo;

d) mantener registros de todas las fallas sospechadas o reales, y de todo mantenimiento preventivo y correctivo;

e) implementar controles apropiados cuando el equipo esté programado para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; someter al personal de mantenimiento a un adecuado acuerdo de confidencialidad;

f) supervisar al personal de mantenimiento al realizar el mantenimiento en el sitio;

g) autorizar y controlar el acceso para el mantenimiento remoto;

h) aplicar medidas de seguridad para activos fuera de las instalaciones (ver7.9) si el equipo que contiene información se retira de las instalaciones para su mantenimiento;

i) cumplir con todos los requisitos de mantenimiento impuestos por el seguro;

j) antes de volver a poner en funcionamiento el equipo después del mantenimiento, inspeccionarlo para asegurarse de que el equipo no haya sido manipulado y funcione correctamente;

k) aplicar medidas para la eliminación segura o la reutilización de equipos (ver7.14) si se determina que el equipo debe desecharse.

Otra información

El equipo incluye componentes técnicos de las instalaciones de procesamiento de información, fuente de alimentación ininterrumpida (UPS) y baterías, generadores de energía, alternadores y convertidores de energía, sistemas y alarmas de detección de intrusión física, detectores de humo, extintores de incendios, aire acondicionado y ascensores.

7.14 Eliminación segura o reutilización de equipos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Seguridad física # Gestión de activos	# Proteccion

Control

Los elementos del equipo que contengan medios de almacenamiento deben verificarse para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Propósito

Para evitar la fuga de información de los equipos que se desecharán o reutilizarán.

Guia

El equipo debe verificarse para garantizar si los medios de almacenamiento están contenidos o no antes de su eliminación o reutilización.

Los medios de almacenamiento que contengan información confidencial o con derechos de autor deben destruirse físicamente o la información debe destruirse, eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar. Mar7.10 para obtener orientación detallada sobre la eliminación segura de medios de almacenamiento y8.10 para obtener orientación sobre la eliminación de información.

Las etiquetas y marcas que identifiquen a la organización o que indiquen la clasificación, el propietario, el sistema o la red deben eliminarse antes de su eliminación, incluida la reventa o la donación a organizaciones benéficas.

La organización debe considerar la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones. Esto depende de factores como:

a) su contrato de arrendamiento para devolver la instalación a su condición original;

b) minimizar el riesgo de dejar los sistemas con información confidencial para el próximo inquilino (por ejemplo, listas de acceso de usuarios, archivos de video o imagen);

c) la capacidad de reutilizar los controles en la siguiente instalación.

Otra información

El equipo dañado que contiene medios de almacenamiento puede requerir una evaluación de riesgos para determinar si los elementos deben destruirse físicamente en lugar de enviarse a reparar o desecharse. La información puede verse comprometida por la eliminación descuidada o la reutilización del equipo.

Además de la eliminación segura del disco, el cifrado de disco completo reduce el riesgo de divulgación de información confidencial cuando el equipo se desecha o se vuelve a implementar, siempre que:

a) el proceso de encriptación es lo suficientemente fuerte y cubre todo el disco (incluido el espacio libre, los archivos de intercambio);

b) las claves criptográficas son lo suficientemente largas para resistir ataques de fuerza bruta;

c) las claves criptográficas se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para obtener más información sobre criptografía, consulte8.24 .

Las técnicas para sobrescribir de forma segura los medios de almacenamiento difieren según la tecnología de los medios de almacenamiento y el nivel de clasificación de la información en los medios de almacenamiento. Las herramientas de sobrescritura deben revisarse para asegurarse de que sean aplicables a la tecnología de los medios de almacenamiento.

Consulte la norma ISO/IEC 27040 para obtener detalles sobre los métodos para desinfectar los medios de almacenamiento.

8 Controles tecnológicos

8.1 Dispositivos de punto final de usuario

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gestión de activos # Información_protección	# Proteccion

Control

La información almacenada, procesada o accesible a través de los dispositivos finales de los usuarios debe protegerse.

Propósito

Para proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.

Guia

General

La organización debe establecer una política específica del tema sobre la configuración y el manejo seguros de los dispositivos de punto final del usuario. La política específica del tema debe comunicarse a todo el personal pertinente y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar o admitir;

b) registro de dispositivos de punto final de usuario;

c) requisitos de protección física;

d) restricción de la instalación de software (p. ej., controlado de forma remota por los administradores del sistema);

e) requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para aplicar actualizaciones (por ejemplo, actualización automática activa);

f) reglas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, que requiera el uso de un cortafuegos personal);

g) controles de acceso;

h) cifrado del dispositivo de almacenamiento;

i) protección contra malware;

j) deshabilitación, borrado o bloqueo remoto;

k) copias de seguridad;

l) uso de servicios web y aplicaciones web;

m) análisis del comportamiento del usuario final (ver8.16);

n) el uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar puertos físicos (por ejemplo, puertos USB);

o) el uso de capacidades de partición, si es compatible con el dispositivo de punto final del usuario, que puede separar de forma segura la información de la organización y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados en el dispositivo.

Se debe considerar si cierta información es tan confidencial que solo se puede acceder a ella a través de los dispositivos de punto final del usuario, pero no se almacena en dichos dispositivos. En tales casos, se pueden requerir protecciones técnicas adicionales en el dispositivo. Por ejemplo, asegurarse de que la descarga de archivos para trabajar sin conexión esté deshabilitada y que el almacenamiento local, como la tarjeta SD, esté deshabilitado.

En la medida de lo posible, las recomendaciones sobre este control deben hacerse cumplir a través de la gestión de la configuración (ver8.9) o herramientas automatizadas.

responsabilidad del usuario

Todos los usuarios deben ser conscientes de los requisitos y procedimientos de seguridad para proteger los dispositivos de punto final de los usuarios, así como de sus responsabilidades para implementar dichas medidas de seguridad. Se debe recomendar a los usuarios que:

a) cerrar sesiones activas y cancelar servicios cuando ya no se necesiten;

b) proteger los dispositivos de punto final del usuario del uso no autorizado con un control físico (p. ej., bloqueo de teclas o bloqueos especiales) y un control lógico (p. ej., acceso con contraseña) cuando no estén en uso; no dejar desatendidos los dispositivos que transportan información comercial importante, confidencial o crítica;

c) usar dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas (por ejemplo, evitar leer información confidencial si las personas pueden leer por detrás, usar filtros de pantalla de privacidad);

d) proteger físicamente los dispositivos de punto final del usuario contra el robo (por ejemplo, en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Debe establecerse un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales (incluidos los seguros) y otros requisitos de seguridad de la organización para casos de robo o pérdida de dispositivos de punto final de usuario.

Uso de dispositivos personales.

Cuando la organización permita el uso de dispositivos personales (a veces conocidos como BYOD), además de la orientación proporcionada en este control, se debe considerar lo siguiente:

a) separación del uso personal y comercial de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos comerciales en un dispositivo privado;

b) proporcionar acceso a la información comercial solo después de que los usuarios hayan reconocido sus deberes (protección física, actualización de software, etc.), renunciar a la propiedad de los datos comerciales, permitir que la organización borre datos de forma remota en caso de robo o pérdida del dispositivo o cuando ya no está autorizado a utilizar el servicio. En tales casos, se debe considerar la legislación de protección de PII;

c) políticas y procedimientos específicos del tema para prevenir disputas relacionadas con los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

d) acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que puede ser impedido por la legislación;

e) acuerdos de licencia de software que son tales que las organizaciones pueden ser responsables de la concesión de licencias de software de cliente en dispositivos de punto final de usuario propiedad privada del personal o usuarios externos.

Conexiones inalámbricas

La organización debería establecer procedimientos para:

a) la configuración de conexiones inalámbricas en dispositivos (p. ej., desactivación de protocolos vulnerables);

b) usar conexiones inalámbricas o por cable con el ancho de banda adecuado de acuerdo con las políticas específicas del tema (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de software).

Otra información

Los controles para proteger la información en los dispositivos de punto final del usuario dependen de si el dispositivo de punto final del usuario se usa solo dentro de las instalaciones seguras y las conexiones de red de la organización, o si está expuesto a mayores amenazas físicas y relacionadas con la red fuera de la organización.

Las conexiones inalámbricas para los dispositivos de punto final del usuario son similares a otros tipos de conexiones de red, pero tienen diferencias importantes que deben tenerse en cuenta al identificar los controles. En particular, la copia de seguridad de la información almacenada en los dispositivos de punto final del usuario a veces puede fallar debido al ancho de banda de red limitado o porque los dispositivos de punto final del usuario no están conectados en los momentos en que se programan las copias de seguridad.

Para algunos puertos USB, como USB-C, no es posible deshabilitar el puerto USB porque se usa para otros fines (por ejemplo, suministro de energía y salida de pantalla).

8.2 Derechos de acceso privilegiado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Capacidad operativa Habilidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_ac-cess_management	# Proteccion

Control

La asignación y el uso de derechos de acceso privilegiado deben restringirse y gestionarse.

Propósito

Para garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiados.

Guia

La asignación de derechos de acceso privilegiado debe controlarse a través de un proceso de autorización de acuerdo con la política de control de acceso específica del tema pertinente (ver5.15). Se debe considerar lo siguiente:

a) identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones);

b) asignar derechos de acceso privilegiado a los usuarios según sea necesario y caso por caso de acuerdo con la política específica del tema sobre control de acceso (ver5.15) (es decir, solo a personas con la competencia necesaria para llevar a cabo actividades que requieren un acceso privilegiado y con base en el requisito mínimo para sus roles funcionales);

c) mantener un proceso de autorización (es decir, determinar quién puede aprobar derechos de acceso privilegiado o no otorgar derechos de acceso privilegiado hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados;

d) definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado;

e) tomar medidas para garantizar que los usuarios conozcan sus derechos de acceso privilegiado y cuándo se encuentran en el modo de acceso privilegiado. Las posibles medidas incluyen el uso de identidades de usuario específicas, configuraciones de interfaz de usuario o incluso equipos específicos;

f) los requisitos de autenticación para los derechos de acceso privilegiado pueden ser más altos que los requisitos para los derechos de acceso normales. Es posible que sea necesario volver a autenticarse o aumentar la autenticación antes de trabajar con derechos de acceso privilegiados;

g) regularmente, y después de cualquier cambio organizacional, revisar a los usuarios que trabajan con derechos de acceso privilegiado para verificar si sus deberes, roles, responsabilidades y competencia aún los califican para trabajar con derechos de acceso privilegiado (ver5.18);

h) establecer reglas específicas para evitar el uso de identificaciones de usuario de administración genéricas (como “root”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de dichas identidades (ver5.17);

i) otorgar acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar derechos de acceso privilegiado de forma permanente. Esto a menudo se conoce como procedimiento de rotura de cristal y, a menudo, se automatiza mediante tecnologías de gestión de acceso privilegiado;

j) registrar todos los accesos privilegiados a los sistemas con fines de auditoría;

k) no compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos. Las identidades se pueden agrupar (p. ej., definiendo un grupo de administradores) para simplificar la gestión de los derechos de acceso privilegiado;

l) usar únicamente identidades con derechos de acceso privilegiado para realizar tareas administrativas y no para tareas generales del día a día [es decir, revisar el correo electrónico, acceder a la web (los usuarios deben tener una identidad de red normal separada para estas actividades)].

Otra información

Los derechos de acceso privilegiado son derechos de acceso proporcionados a una identidad, un rol o un proceso que permite realizar actividades que los usuarios o procesos típicos no pueden realizar. Los roles de administrador del sistema generalmente requieren derechos de acceso privilegiado.

El uso inapropiado de los privilegios del administrador del sistema (cualquier característica o instalación de un sistema de información que permita al usuario anular los controles del sistema o de la aplicación) es un factor importante que contribuye a las fallas o violaciones de los sistemas.

Se puede encontrar más información relacionada con la gestión de acceso y la gestión segura del acceso a la información y los recursos de tecnologías de la información y las comunicaciones en ISO/IEC 29146.

8.3 Restricción de acceso a la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica del tema establecida sobre el control de acceso.

Propósito

Para garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Guia

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con las políticas específicas del tema establecidas. Se debe considerar lo siguiente para respaldar los requisitos de restricción de acceso:

a) no permitir el acceso a información sensible por parte de usuarios con identidades desconocidas o de forma anónima. El acceso público o anónimo solo debe otorgarse a lugares de almacenamiento que no contengan información confidencial;

b) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

c) controlar a qué datos puede acceder un usuario en particular;

d) controlar qué identidades o grupo de identidades tienen qué acceso, como lectura, escritura, eliminación y ejecución;

e) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicaciones o sistemas.

Además, se deben considerar técnicas y procesos de gestión de acceso dinámico para proteger información confidencial que tiene un gran valor para la organización cuando la organización:

a) necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) quiere compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella;

c) quiere gestionar dinámicamente, en tiempo real, el uso y distribución de dicha información;

d) quiere proteger dicha información contra cambios no autorizados, copia y distribución (incluida la impresión);

e) quiere monitorear el uso de la información;

f) quiere registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura.

Las técnicas de gestión de acceso dinámico deben proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer reglas sobre la gestión del acceso dinámico en función de casos de uso específicos considerando:

1) otorgar permisos de acceso en función de la identidad, el dispositivo, la ubicación o la aplicación;

2) aprovechar el esquema de clasificación para determinar qué información debe protegerse con técnicas de gestión de acceso dinámico;

b) establecer procesos operativos, de seguimiento y de presentación de informes e infraestructura técnica de apoyo.

Los sistemas de gestión de acceso dinámico deben proteger la información mediante:

a) exigir autenticación, credenciales apropiadas o un certificado para acceder a la información;

b) restringir el acceso, por ejemplo, a un período de tiempo específico (por ejemplo, después de una fecha dada o hasta una fecha particular);

c) usar cifrado para proteger la información;

d) definir los permisos de impresión de la información;

e) registrar quién accede a la información y cómo se utiliza la información;

f) generar alertas si se detectan intentos de mal uso de la información.

Otra información

Las técnicas de gestión de acceso dinámico y otras tecnologías de protección de información dinámica pueden respaldar la protección de la información incluso cuando los datos se comparten más allá de la organización de origen, donde los controles de acceso tradicionales no se pueden aplicar. Se puede aplicar a documentos, correos electrónicos u otros archivos que contengan información para limitar quién puede acceder al contenido y de qué manera. Puede ser a nivel granular y adaptarse a lo largo del ciclo de vida de la información.

Las técnicas de gestión de acceso dinámico no reemplazan la gestión de acceso clásica [p. ej., el uso de listas de control de acceso (ACL)], pero pueden agregar más factores de condicionalidad, evaluación en tiempo real, reducción de datos justo a tiempo y otras mejoras que pueden ser útiles para el información más sensible. Ofrece una forma de controlar el acceso fuera del entorno de la organización. La respuesta a incidentes se puede respaldar con técnicas de gestión de acceso dinámico, ya que los permisos se pueden modificar o revocar en cualquier momento.

En ISO/IEC 29146 se proporciona información adicional sobre un marco para la gestión de acceso.

8.4 Acceso al código fuente

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Identidad_y_acceso_ administración #Aplicación_seguridad # Secure_configura-ción	# Proteccion

Control

El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe administrarse adecuadamente.

Propósito

Para evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

Guia

El acceso al código fuente y elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas y entornos de prueba) debe controlarse estrictamente.

Para el código fuente, esto se puede lograr controlando el almacenamiento central de dicho código, preferiblemente en el sistema de gestión de código fuente.

El acceso de lectura y el acceso de escritura al código fuente pueden diferir según la función del personal. Por ejemplo, el acceso de lectura al código fuente se puede proporcionar ampliamente dentro de la organización, pero el acceso de escritura al código fuente

solo está disponible para personal privilegiado o propietarios designados. Cuando los componentes del código son utilizados por varios desarrolladores dentro de una organización, se debe implementar el acceso de lectura a un repositorio de código centralizado. Además, si dentro de una organización se utiliza código fuente abierto o componentes de código de terceros, el acceso de lectura a dichos repositorios de código externos puede proporcionarse ampliamente. Sin embargo, el acceso de escritura aún debe estar restringido.

Se deben considerar las siguientes pautas para controlar el acceso a las bibliotecas de fuentes de programas a fin de reducir el potencial de corrupción de los programas de computadora:

a) administrar el acceso al código fuente del programa y las bibliotecas fuente del programa de acuerdo con los procedimientos establecidos;

b) otorgar acceso de lectura y escritura al código fuente en función de las necesidades comerciales y administrado para abordar los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos;

c) actualización del código fuente y elementos asociados y otorgamiento de acceso al código fuente de acuerdo con los procedimientos de control de cambios (ver8.32) y solo realizarlo después de haber recibido la autorización correspondiente;

d) no otorgar a los desarrolladores acceso directo al repositorio del código fuente, sino a través de herramientas para desarrolladores que controlan las actividades y autorizaciones en el código fuente;

e) mantener las listas de programas en un entorno seguro, donde el acceso de lectura y escritura debe administrarse y asignarse adecuadamente;

f) mantener un registro de auditoría de todos los accesos y de todos los cambios en el código fuente.

Si se pretende publicar el código fuente del programa, se deben considerar controles adicionales para garantizar su integridad (p. ej., firma digital).

Otra información

Si el acceso al código fuente no se controla adecuadamente, el código fuente puede modificarse o algunos datos en el entorno de desarrollo (por ejemplo, copias de datos de producción, detalles de configuración) pueden ser recuperados por personas no autorizadas.

8.5 Autenticación segura

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

Control

Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

Propósito

Para garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.

Guia

Se debe elegir una técnica de autenticación adecuada para corroborar la identidad reclamada de un usuario, software, mensajes y otras entidades.

La fuerza de la autenticación debe ser adecuada para la clasificación de la información a la que se accede. Cuando se requiera una fuerte autenticación y verificación de identidad, los métodos de autenticación

Se deben utilizar alternativas a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos.

La información de autenticación debe ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información crítica (también conocida como autenticación de múltiples factores). El uso de una combinación de múltiples factores de autenticación, como lo que sabe, lo que tiene y lo que es, reduce las posibilidades de accesos no autorizados. La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, en función de reglas y patrones predefinidos, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual.

La información de autenticación biométrica debe invalidarse si alguna vez se ve comprometida. La autenticación biométrica puede no estar disponible según las condiciones de uso (p. ej., humedad o envejecimiento). Para prepararse para estos problemas, la autenticación biométrica debe ir acompañada de al menos una técnica de autenticación alternativa.

El procedimiento para iniciar sesión en un sistema o aplicación debe estar diseñado para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión deben implementarse teniendo en cuenta lo siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito para evitar proporcionar asistencia innecesaria a un usuario no autorizado;

b) exhibir un aviso general advirtiendo que el sistema o la aplicación o el servicio solo deben ser accedidos por usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayuden a un usuario no autorizado (por ejemplo, si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta);

d) validar la información de inicio de sesión solo al completar todos los datos de entrada;

e) protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas [p. ej., usar la prueba de Turing pública completamente automatizada para diferenciar computadoras y humanos (CAPTCHA), requerir el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores];

f) registrar intentos fallidos y exitosos;

g) generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión (p. ej., enviar una alerta al usuario ya los administradores del sistema de la organización cuando se alcanza un cierto número de intentos de contraseña incorrectos);

h) mostrar o enviar la siguiente información en un canal separado al completar un inicio de sesión exitoso:

1) fecha y hora del inicio de sesión exitoso anterior;

2) detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso;

i) no mostrar una contraseña en texto claro cuando se ingresa; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por ejemplo, por razones de accesibilidad o para evitar el bloqueo de usuarios debido a errores repetidos);

j) no transmitir contraseñas en texto claro a través de una red para evitar ser capturado por un programa "sniffer" de la red;

k) finalizar sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo, como áreas públicas o externas fuera de la gestión de seguridad de la organización o en dispositivos de punto final de usuario;

l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Otra información

Se puede encontrar información adicional sobre la garantía de autenticación de entidades en ISO / IEC 29115.

8.6 Gestión de la capacidad

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Integridad # Disponibilidad	# Identificar # Proteger # Detectar	# Continuidad	# Gobernanza_y_ Ecosistema # Protección ción

Control

El uso de los recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.

Propósito

Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

Guia

Deben identificarse los requisitos de capacidad para las instalaciones de procesamiento de información, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la importancia comercial de los sistemas y procesos en cuestión.

Se debe aplicar el ajuste y la supervisión del sistema para garantizar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

La organización debería realizar pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema disponible para cumplir con los requisitos de rendimiento máximo.

Deben establecerse controles de detección para indicar los problemas a su debido tiempo.

Las proyecciones de los futuros requisitos de capacidad deben tener en cuenta los nuevos requisitos del negocio y del sistema y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.

Se debe prestar especial atención a cualquier recurso con largos plazos de entrega o altos costos. Por lo tanto, los gerentes, propietarios de servicios o productos deben monitorear la utilización de los recursos clave del sistema.

Los gerentes deben usar la información de capacidad para identificar y evitar posibles limitaciones de recursos y dependencias del personal clave que pueden representar una amenaza para la seguridad del sistema o los servicios y planificar la acción adecuada.

Se puede lograr proporcionar capacidad suficiente aumentando la capacidad o reduciendo la demanda. Se debe considerar lo siguiente para aumentar la capacidad:

a) contratación de nuevo personal;

b) obtención de nuevas instalaciones o espacio;

c) adquirir sistemas de procesamiento, memoria y almacenamiento más potentes;

d) hacer uso de la computación en la nube, que tiene características inherentes que abordan directamente cuestiones de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión y reducción bajo demanda de los recursos disponibles para aplicaciones y servicios particulares.

Se debe considerar lo siguiente para reducir la demanda de los recursos de la organización:

a) eliminación de datos obsoletos (espacio en disco);

b) eliminación de registros impresos que tienen su período de retención (liberar espacio en estanterías);

c) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos;

d) optimizar procesos por lotes y cronogramas;

e) optimizar el código de la aplicación o las consultas de la base de datos;

f) denegar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos (por ejemplo, transmisión de video).

Se debe considerar un plan de gestión de capacidad documentado para los sistemas de misión crítica.

Otra información

Para obtener más detalles sobre la elasticidad y la escalabilidad de la computación en la nube, consulte ISO/IEC TS 23167.

8.7 Protección contra malware

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective # Correctivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# Sistema_y_red_ seguridad # Information_protec-ción	# Proteccion # Defensa

Control

La protección contra el malware debe implementarse y respaldarse mediante la conciencia adecuada del usuario.

Propósito

Para garantizar que la información y otros activos asociados estén protegidos contra malware.

Guia

La protección contra el malware debe basarse en software de detección y reparación de malware, conciencia de seguridad de la información, acceso al sistema adecuado y controles de gestión de cambios. El uso de software de detección y reparación de malware por sí solo no suele ser adecuado. Se debe considerar la siguiente orientación:

a) implementar reglas y controles que prevengan o detecten el uso de software no autorizado [por ejemplo, lista de aplicaciones permitidas (es decir, usar una lista que proporcione aplicaciones permitidas)] (ver8.19 y8.32);

b) implementar controles que eviten o detecten el uso de sitios web maliciosos conocidos o sospechosos (por ejemplo, listas de bloqueo);

c) reducir las vulnerabilidades que pueden ser explotadas por malware [por ejemplo, a través de la gestión técnica de vulnerabilidades (ver8.8 y8.19)];

d) llevar a cabo una validación automatizada periódica del software y el contenido de datos de los sistemas, especialmente para los sistemas que soportan procesos comerciales críticos; investigar la presencia de archivos no aprobados o enmiendas no autorizadas;

e) establecer medidas de protección contra los riesgos asociados con la obtención de archivos y software ya sea desde oa través de redes externas o en cualquier otro medio;

f) instalar y actualizar regularmente software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónico. Realización de escaneos regulares que incluyen:

1) escanear cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso;

2) escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso. Llevar a cabo este escaneo en diferentes lugares (por ejemplo, en servidores de correo electrónico, computadoras de escritorio) y al ingresar a la red de la organización;

3) escanear páginas web en busca de malware cuando se accede a ellas;

g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y considerando:

1) principios de defensa en profundidad donde serían más efectivos. Por ejemplo, esto puede conducir a la detección de malware en una puerta de enlace de red (en varios protocolos de aplicación, como correo electrónico, transferencia de archivos y web), así como en servidores y dispositivos de punto final de usuario;

2) las técnicas evasivas de los atacantes (p. ej., el uso de archivos cifrados) para entregar malware o el uso de protocolos de cifrado para transmitir malware;

h) tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el malware;

i) implementar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra malware provoca la interrupción de las operaciones normales;

j) preparar planes de continuidad comercial apropiados para recuperarse de ataques de malware, incluidas todas las copias de seguridad de datos y software necesarias (incluidas las copias de seguridad en línea y fuera de línea) y las medidas de recuperación (ver8.13);

k) aislar ambientes donde puedan ocurrir consecuencias catastróficas;

l) definir procedimientos y responsabilidades para tratar la protección contra malware en los sistemas, incluida la capacitación en su uso, informes y recuperación de ataques de malware;

m) brindar conciencia o capacitación (ver6.3) a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados con malware [la información recopilada en n) y o) puede usarse para garantizar que la conciencia y la capacitación se mantengan actualizadas];

n) implementar procedimientos para recopilar regularmente información sobre nuevo malware, como suscribirse a listas de correo o revisar sitios web relevantes;

o) verificar que la información relacionada con el malware, como los boletines de advertencia, provenga de fuentes calificadas y acreditadas (por ejemplo, sitios de Internet confiables o proveedores de software de detección de malware) y que sea precisa e informativa.

Otra información

No siempre es posible instalar software que proteja contra malware en algunos sistemas (por ejemplo, algunos sistemas de control industrial). Algunas formas de malware infectan los sistemas operativos y el firmware de la computadora, de modo que los controles de malware comunes no pueden limpiar el sistema y es necesario volver a crear una imagen completa del software del sistema operativo y, a veces, del firmware de la computadora para volver a un estado seguro.

8.8 Gestión de vulnerabilidades técnicas

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar # Proteger	# amenaza_y_ vulnerabilidad_ administración	# Gobernanza_y_Ecosistema # Protección #Defensa

Control

Debería obtenerse información sobre las vulnerabilidades técnicas de los sistemas de información en uso, debería evaluarse la exposición de la organización a tales vulnerabilidades y deberían tomarse las medidas apropiadas.

Propósito

Para prevenir la explotación de vulnerabilidades técnicas.

Guia

Identificación de vulnerabilidades técnicas

La organización debe tener un inventario preciso de activos (ver5.9 para5.14) como requisito previo para una gestión técnica eficaz de la vulnerabilidad; el inventario debe incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) dentro de la organización responsable del software.

Para identificar vulnerabilidades técnicas, la organización debe considerar:

a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de vulnerabilidades, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidades, la actualización, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;

b) para software y otras tecnologías (basado en la lista de inventario de activos, véase5.9), identificando los recursos de información que se utilizarán para identificar vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles;

c) exigir a los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el manejo y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables (véase5.20);

d) usar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si la reparación de vulnerabilidades fue exitosa;

e) realizar pruebas de penetración planificadas, documentadas y repetibles o evaluaciones de vulnerabilidad por parte de personas competentes y autorizadas para respaldar la identificación de vulnerabilidades. Tener precaución ya que tales actividades pueden comprometer la seguridad del sistema;

f) rastrear el uso de bibliotecas de terceros y código fuente en busca de vulnerabilidades. Esto debe incluirse en la codificación segura (ver8.28).

La organización debe desarrollar procedimientos y capacidades para:

a) detectar la existencia de vulnerabilidades en sus productos y servicios incluyendo cualquier componente externo utilizado en estos;

b) recibir informes de vulnerabilidad de fuentes internas o externas.

La organización debe proporcionar un punto de contacto público como parte de una política específica de un tema sobre la divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar problemas. La organización debería establecer procedimientos de notificación de vulnerabilidades, formularios de notificación en línea y hacer uso de inteligencia de amenazas o foros de intercambio de información apropiados. La organización también debe considerar los programas de recompensas por errores.

donde las recompensas se ofrecen como un incentivo para ayudar a las organizaciones a identificar vulnerabilidades para remediarlas adecuadamente. La organización también debería compartir información con los organismos competentes de la industria u otras partes interesadas.

Evaluación de vulnerabilidades técnicas

Para evaluar las vulnerabilidades técnicas identificadas, se debe considerar la siguiente guía:

a) analizar y verificar los informes para determinar qué actividad de respuesta y remediación se necesita;

b) una vez identificada una potencial vulnerabilidad técnica, identificar los riesgos asociados y las acciones a tomar. Tales acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles.

Tomar las medidas apropiadas para abordar las vulnerabilidades técnicas

Se debe implementar un proceso de administración de actualizaciones de software para garantizar que se instalen los parches aprobados y las actualizaciones de aplicaciones más actualizados para todo el software autorizado. Si es necesario realizar cambios, se debe conservar el software original y aplicar los cambios a una copia designada. Todos los cambios deben probarse y documentarse por completo, de modo que puedan volver a aplicarse, si es necesario, a futuras actualizaciones de software. Si es necesario, las modificaciones deben ser probadas y validadas por un organismo de evaluación independiente.

Se debe considerar la siguiente orientación para abordar las vulnerabilidades técnicas:

a) tomar medidas apropiadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un cronograma para responder a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

b) dependiendo de la urgencia con la que se deba abordar una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión del cambio (ver8.32) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (ver5.26);

c) utilizar únicamente actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización);

d) probar y evaluar las actualizaciones antes de instalarlas para garantizar que sean efectivas y no produzcan efectos secundarios que no se puedan tolerar [es decir, si hay una actualización disponible, evaluar los riesgos asociados con la instalación de la actualización (los riesgos que plantea la vulnerabilidad debe compararse con el riesgo de instalar la actualización)];

e) abordar primero los sistemas de alto riesgo;

f) desarrollar soluciones (por lo general, actualizaciones o parches de software);

g) prueba para confirmar si la remediación o mitigación es efectiva;

h) proporcionar mecanismos para verificar la autenticidad de la remediación;

i) si no hay actualización disponible o no se puede instalar la actualización, considerando otros controles, tales como:

1) aplicar cualquier solución alternativa sugerida por el proveedor de software u otras fuentes relevantes;

2) apagar servicios o capacidades relacionadas con la vulnerabilidad;

3) adaptar o agregar controles de acceso (por ejemplo, cortafuegos) en los límites de la red (ver8.20 para8.22);

4) proteger los sistemas, dispositivos o aplicaciones vulnerables de los ataques mediante la implementación de filtros de tráfico adecuados (a veces denominados parches virtuales);

5) aumentar el monitoreo para detectar ataques reales;

6) sensibilización sobre la vulnerabilidad.

Para el software adquirido, si los proveedores publican regularmente información sobre actualizaciones de seguridad para su software y brindan una instalación para instalar dichas actualizaciones automáticamente, la organización debe decidir si usar la actualización automática o no.

Otras Consideraciones

Se debe mantener un registro de auditoría para todos los pasos realizados en la gestión de vulnerabilidades técnicas.

El proceso de gestión de vulnerabilidades técnicas debe ser monitoreado y evaluado regularmente para asegurar su efectividad y eficiencia.

Un proceso eficaz de gestión de vulnerabilidades técnicas debe estar alineado con las actividades de gestión de incidentes, para comunicar datos sobre vulnerabilidades a la función de respuesta a incidentes y proporcionar procedimientos técnicos que se llevarán a cabo en caso de que ocurra un incidente.

Cuando la organización utiliza un servicio en la nube proporcionado por un proveedor de servicios en la nube externo, el proveedor de servicios en la nube debe garantizar la gestión de la vulnerabilidad técnica de los recursos del proveedor de servicios en la nube. Las responsabilidades del proveedor de servicios en la nube para la gestión de vulnerabilidades técnicas deben ser parte del acuerdo de servicios en la nube y esto debe incluir procesos para informar las acciones del proveedor de servicios en la nube relacionadas con las vulnerabilidades técnicas (ver5.23). Para algunos servicios en la nube, existen responsabilidades respectivas para el proveedor del servicio en la nube y el cliente del servicio en la nube. Por ejemplo, el cliente del servicio en la nube es responsable de la gestión de vulnerabilidades de sus propios activos utilizados para los servicios en la nube.

Otra información

La gestión de vulnerabilidades técnicas puede verse como una subfunción de la gestión de cambios y, como tal, puede aprovechar los procesos y procedimientos de gestión de cambios (ver8.32).

Existe la posibilidad de que una actualización no resuelva el problema adecuadamente y tenga efectos secundarios negativos. Además, en algunos casos, la desinstalación de una actualización no se puede lograr fácilmente una vez que se ha aplicado la actualización.

Si no es posible realizar pruebas adecuadas de las actualizaciones (por ejemplo, debido a los costos o la falta de recursos), se puede considerar un retraso en la actualización para evaluar los riesgos asociados, según la experiencia informada por otros usuarios. El uso de ISO/IEC 27031 puede ser beneficioso.

Cuando se produzcan parches o actualizaciones de software, la organización puede considerar proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados sin necesidad de intervención por parte del cliente o el usuario. Si se ofrece un proceso de actualización automática, puede permitir que el cliente o usuario elija una opción para desactivar la actualización automática o controlar el tiempo de instalación de la actualización.

Cuando el proveedor proporciona un proceso de actualización automatizado y las actualizaciones se pueden instalar en los sistemas o productos afectados sin necesidad de intervención, la organización determina si aplica el proceso automatizado o no. Una razón para no elegir la actualización automática es mantener el control sobre cuándo se realiza la actualización. Por ejemplo, un software utilizado para una operación comercial no se puede actualizar hasta que la operación se haya completado.

Una debilidad del análisis de vulnerabilidades es que es posible que no tenga en cuenta completamente la defensa en profundidad: dos contramedidas que siempre se invocan en secuencia pueden tener vulnerabilidades que están enmascaradas por las fortalezas de la otra. La contramedida compuesta no es vulnerable, mientras que un escáner de vulnerabilidades puede informar que ambos componentes son vulnerables. Por lo tanto, la organización debe tener cuidado al revisar y actuar sobre los informes de vulnerabilidad.

Muchas organizaciones suministran software, sistemas, productos y servicios no solo dentro de la organización sino también a partes interesadas como clientes, socios u otros usuarios. Estos software, sistemas, productos y servicios pueden tener vulnerabilidades de seguridad de la información que afecten la seguridad de los usuarios.

Las organizaciones pueden publicar la remediación y divulgar información sobre las vulnerabilidades a los usuarios (generalmente a través de un aviso público) y proporcionar la información adecuada para los servicios de base de datos de vulnerabilidades de software.

Para obtener más información relacionada con la gestión de vulnerabilidades técnicas cuando se utiliza la computación en la nube, consulte la serie ISO/IEC 19086 e ISO/IEC 27017.

ISO/IEC 29147 proporciona información detallada sobre cómo recibir informes de vulnerabilidad y publicar avisos de vulnerabilidad. ISO/IEC 30111 proporciona información detallada sobre el manejo y la resolución de vulnerabilidades informadas.

8.9 Gestión de la configuración

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# configuración_segura	# Proteccion

Control

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

Propósito

Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se altere por cambios no autorizados o incorrectos.

Guia

General

La organización debe definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para sistemas recién instalados, así como para sistemas operativos durante su vida útil.

Deben existir roles, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración.

Plantillas estándar

Deben definirse plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) usar orientación disponible públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad independientes);

b) considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad;

c) respaldar la política de seguridad de la información de la organización, las políticas específicas del tema, las normas y otros requisitos de seguridad;

d) considerar la factibilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas deben revisarse periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades, o cuando se introduzcan nuevas versiones de software o hardware.

Se debe considerar lo siguiente para establecer plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) deshabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a poderosos programas de utilidades y configuraciones de parámetros del host;

e) sincronización de relojes;

f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad predeterminada;

g) invocar las instalaciones de tiempo de espera que cierran automáticamente la sesión de los dispositivos informáticos después de un período predeterminado de inactividad;

h) verificar que se hayan cumplido los requisitos de la licencia (ver5.32).

Administrar configuraciones

Las configuraciones establecidas de hardware, software, servicios y redes deben registrarse y debe mantenerse un registro de todos los cambios de configuración. Estos registros deben almacenarse de forma segura. Esto se puede lograr de varias maneras, como bases de datos de configuración o plantillas de configuración.

Los cambios en las configuraciones deben seguir el proceso de gestión de cambios (ver8.32).

Los registros de configuración pueden contener según corresponda:

a) información actualizada del propietario o punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de la plantilla de configuración;

d) relación con configuraciones de otros activos.

Monitoreo de configuraciones

Las configuraciones deben monitorearse con un conjunto integral de herramientas de administración del sistema (p. ej., utilidades de mantenimiento, soporte remoto, herramientas de administración empresarial, software de copia de seguridad y restauración) y deben revisarse periódicamente para verificar los ajustes de configuración, evaluar la seguridad de las contraseñas y evaluar las actividades realizadas. Las configuraciones reales se pueden comparar con las plantillas de destino definidas. Cualquier desviación debe abordarse, ya sea mediante la aplicación automática de la configuración objetivo definida o mediante el análisis manual de la desviación seguido de acciones correctivas.

Otra información

La documentación de los sistemas a menudo registra detalles sobre la configuración tanto del hardware como del software.

El endurecimiento del sistema es una parte típica de la gestión de la configuración.

La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

La automatización suele ser más eficaz para gestionar la configuración de seguridad (por ejemplo, utilizando la infraestructura como código).

Las plantillas de configuración y los destinos pueden ser información confidencial y, en consecuencia, deben protegerse contra el acceso no autorizado.

8.10 Eliminación de información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	#Información_protección # Legal_and_compliance	# Proteccion

Control

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.

Propósito

Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.

Guia

General

La información confidencial no debe conservarse más tiempo del necesario para reducir el riesgo de divulgación no deseada.

Al eliminar información sobre sistemas, aplicaciones y servicios, se debe considerar lo siguiente:

a) seleccionar un método de eliminación (p. ej., sobrescritura electrónica o borrado criptográfico) de acuerdo con los requisitos comerciales y teniendo en cuenta las leyes y reglamentos pertinentes;

b) registrar los resultados de la eliminación como prueba;

c) al utilizar proveedores de servicios de eliminación de información, obtener evidencia de la eliminación de información de ellos.

Cuando terceros almacenen la información de la organización en su nombre, la organización debe considerar la inclusión de requisitos sobre la eliminación de información en los acuerdos de terceros para hacerlos cumplir durante y después de la finalización de dichos servicios.

Métodos de eliminación

De acuerdo con la política de retención de datos específica del tema de la organización y teniendo en cuenta la legislación y las reglamentaciones pertinentes, la información confidencial debe eliminarse cuando ya no sea necesaria:

a) configurar sistemas para destruir información de forma segura cuando ya no se necesite (por ejemplo, después de un período definido sujeto a la política específica del tema sobre retención de datos o por solicitud de acceso del sujeto);

b) eliminar versiones obsoletas, copias y archivos temporales dondequiera que se encuentren;

c) usar un software de eliminación seguro y aprobado para eliminar información de forma permanente para ayudar a garantizar que la información no se pueda recuperar mediante el uso de herramientas forenses o de recuperación especializadas;

d) usar proveedores aprobados y certificados o servicios de disposición segura;

e) utilizar mecanismos de eliminación apropiados para el tipo de medio de almacenamiento que se va a eliminar (p. ej., desmagnetización de unidades de disco duro y otros medios de almacenamiento magnético).

Cuando se utilizan servicios en la nube, la organización debe verificar si el método de eliminación proporcionado por el proveedor de servicios en la nube es aceptable y, de ser así, la organización debe usarlo o solicitar que el proveedor de servicios en la nube elimine la información. Estos procesos de eliminación deben automatizarse en

de acuerdo con las políticas específicas del tema, cuando estén disponibles y sean aplicables. Dependiendo de la confidencialidad de la información eliminada, los registros pueden rastrear o verificar que estos procesos de eliminación hayan ocurrido.

Para evitar la exposición involuntaria de información confidencial cuando el equipo se devuelve a los proveedores, la información confidencial debe protegerse eliminando los almacenamientos auxiliares (por ejemplo, unidades de disco duro) y la memoria antes de que el equipo abandone las instalaciones de la organización.

Teniendo en cuenta que la eliminación segura de algunos dispositivos (por ejemplo, teléfonos inteligentes) solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo, "restaurar la configuración de fábrica"), la organización debe elegir el método apropiado de acuerdo con la clasificación de la información manejada por tales dispositivos.

Medidas de control descritas en7.14 debe aplicarse para destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene.

Un registro oficial de borrado de información es útil a la hora de analizar la causa de un posible evento de fuga de información.

Otra información

La información sobre la eliminación de datos de usuario en los servicios en la nube se puede encontrar en ISO / IEC 27017.

La información sobre la eliminación de PII se puede encontrar en ISO / IEC 27555.

8.11 Enmascaramiento de datos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad	# Proteger	# Información_protección	# Proteccion

Control

El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.

Propósito

Limitar la exposición de datos confidenciales, incluida la PII, y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

Guia

Cuando la protección de datos confidenciales (por ejemplo, PII) sea una preocupación, la organización debe considerar ocultar dichos datos mediante el uso de técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar la PII, disfrazar la verdadera identidad de los titulares de la PII u otra información confidencial, y desconectar el vínculo entre la PII y la identidad del titular de la PII o el vínculo entre otra información confidencial.

Cuando se utilicen técnicas de seudonimización o anonimización, se debe verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados. La anonimización de datos debe considerar todos los elementos de la información sensible para ser efectivos. A modo de ejemplo, si no se considera adecuadamente, una persona puede ser identificada incluso si los datos que pueden identificar directamente a esa persona se anonimizan, por la presencia de otros datos que permiten identificar a la persona indirectamente.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

a) encriptación (que requiere que los usuarios autorizados tengan una clave);

b) anular o eliminar caracteres (evitando que los usuarios no autorizados vean los mensajes completos);

c) números y fechas variables;

d) sustitución (cambiar un valor por otro para ocultar datos sensibles);

e) reemplazar valores con su hash.

Se debe considerar lo siguiente al implementar técnicas de enmascaramiento de datos:

a) no otorgar a todos los usuarios acceso a todos los datos, por lo tanto, diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario;

b) hay casos en los que algunos datos no deberían ser visibles para el usuario para algunos registros de un conjunto de datos; en este caso, diseñar e implementar un mecanismo para la ofuscación de datos (por ejemplo, si un paciente no quiere que el personal del hospital pueda ver todos sus registros, incluso en caso de emergencia, entonces el personal del hospital recibe datos parcialmente ofuscados y los datos solo pueden ser accedidos por personal con roles específicos si contienen información útil para un tratamiento adecuado);

c) cuando los datos están ofuscados, dando al director de PII la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados (ofuscación de la ofuscación; esto se usa en los centros de salud, por ejemplo, si el paciente no quiere que el personal vea esa información confidencial). se ha ofuscado información como embarazos o resultados de análisis de sangre);

d) cualquier requisito legal o reglamentario (p. ej., exigir el enmascaramiento de la información de las tarjetas de pago durante el procesamiento o el almacenamiento).

Se debe tener en cuenta lo siguiente al utilizar el enmascaramiento de datos, la seudonimización o la anonimización:

a) nivel de fuerza del enmascaramiento de datos, seudonimización o anonimización según el uso de los datos procesados;

b) controles de acceso a los datos procesados;

c) acuerdos o restricciones en el uso de los datos procesados;

d) prohibir cotejar los datos procesados con otra información para identificar al principal de la PII;

e) realizar un seguimiento del suministro y recepción de los datos tratados.

Otra información

La anonimización altera irreversiblemente la PII de tal manera que el principal de la PII ya no se puede identificar directa o indirectamente.

La seudonimización reemplaza la información de identificación con un alias. El conocimiento del algoritmo (a veces denominado "información adicional") utilizado para realizar la seudonimización permite al menos alguna forma de identificación del principal de PII. Por lo tanto, dicha “información adicional” debe mantenerse separada y protegida.

Si bien la seudonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útiles en la investigación estadística.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos confidenciales. El enmascaramiento de datos puede ser estático (cuando los elementos de datos están enmascarados en la base de datos original), dinámico (usando automatización y reglas para proteger los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Las funciones hash se pueden utilizar para anonimizar la PII. Para evitar ataques de enumeración, siempre deben combinarse con una función salt.

La PII en los identificadores de recursos y sus atributos [por ejemplo, nombres de archivo, localizadores uniformes de recursos (URL)] debe evitarse o anonimizarse adecuadamente.

En ISO/IEC 27018 se proporcionan controles adicionales relacionados con la protección de PII en nubes públicas.

Información adicional sobre técnicas de desidentificación está disponible en ISO/IEC 20889.

8.12 Prevención de fuga de datos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad	# Proteger #Detectar	#Información_protección	# Proteccion # Defensa

Control

Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

Propósito

Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Guia

La organización debería considerar lo siguiente para reducir el riesgo de fuga de datos:

a) identificar y clasificar la información para protegerla contra fugas (p. ej., información personal, modelos de precios y diseños de productos);

b) monitorear los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos portátiles de almacenamiento);

c) actuar para evitar que se filtre información (p. ej., poner en cuarentena los correos electrónicos que contengan información confidencial).

Las herramientas de prevención de fuga de datos deben utilizarse para:

a) identificar y monitorear información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados en el sistema de un usuario);

b) detectar la divulgación de información confidencial (p. ej., cuando la información se carga en servicios en la nube de terceros no confiables o se envía por correo electrónico);

c) bloquear las acciones de los usuarios o las transmisiones de la red que expongan información confidencial (p. ej., impedir que se copien las entradas de la base de datos en una hoja de cálculo).

La organización debe determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización. Si ese es el caso, la organización debe implementar tecnología como herramientas de prevención de fuga de datos o la configuración de herramientas existentes que permitan a los usuarios ver y manipular datos almacenados de forma remota pero evitar copiar y pegar fuera del control de la organización.

Si se requiere la exportación de datos, se debe permitir que el propietario de los datos apruebe la exportación y responsabilice a los usuarios por sus acciones.

La toma de capturas de pantalla o fotografías de la pantalla debe abordarse a través de los términos y condiciones de uso, capacitación y auditoría.

Cuando se realiza una copia de seguridad de los datos, se debe tener cuidado para garantizar que la información confidencial esté protegida mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

También se debe considerar la prevención de fuga de datos para protegerse contra las acciones de inteligencia de un adversario de obtener información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o cualquier otra) que puede ser de interés para el espionaje o puede ser crítica para la comunidad. . los

Las acciones de prevención de fuga de datos deben estar orientadas a confundir las decisiones del adversario, por ejemplo, reemplazando información auténtica con información falsa, ya sea como una acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes.

Otra información

Las herramientas de prevención de fuga de datos están diseñadas para identificar datos, monitorear el uso y movimiento de datos y tomar medidas para evitar la fuga de datos (por ejemplo, alertar a los usuarios sobre su comportamiento riesgoso y bloquear la transferencia de datos a dispositivos portátiles de almacenamiento).

La prevención de la fuga de datos involucra inherentemente el monitoreo de las comunicaciones del personal y las actividades en línea y, por extensión, los mensajes de terceros, lo que genera inquietudes legales que deben tenerse en cuenta antes de implementar las herramientas de prevención de la fuga de datos. Existe una variedad de legislación relacionada con la privacidad, la protección de datos, el empleo, la interceptación de datos y las telecomunicaciones que es aplicable al monitoreo y procesamiento de datos en el contexto de la prevención de fugas de datos.

La prevención de la fuga de datos puede estar respaldada por controles de seguridad estándar, como políticas específicas de un tema sobre el control de acceso y la gestión segura de documentos (consulte5.12 y5.15).

8.13 Copia de seguridad de la información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Correctivo	# Integridad # Disponibilidad	# recuperar	# Continuidad	# Proteccion

Control

Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente de acuerdo con la política de respaldo específica del tema acordada.

Propósito

Para permitir la recuperación de la pérdida de datos o sistemas.

Guia

Se debe establecer una política de respaldo específica del tema para abordar los requisitos de seguridad de la información y retención de datos de la organización.

Se deben proporcionar instalaciones de respaldo adecuadas para garantizar que toda la información y el software esenciales se puedan recuperar después de un incidente, falla o pérdida de medios de almacenamiento.

Se deben desarrollar e implementar planes sobre cómo la organización respaldará la información, el software y los sistemas, para abordar la política específica del tema sobre respaldo.

Al diseñar un plan de respaldo, se deben tener en cuenta los siguientes elementos:

a) la producción de registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados;

b) reflejar los requisitos comerciales de la organización (p. ej., el objetivo del punto de recuperación, véase 5.30), los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización en la medida (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de las copias de seguridad;

c) almacenar las copias de seguridad en una ubicación remota segura y protegida, a una distancia suficiente para escapar de cualquier daño de un desastre en el sitio principal;

d) dar a la información de respaldo un nivel adecuado de protección física y ambiental (ver Cláusula 7 y 8.1) consistente con los estándares aplicados en el sitio principal;

e) probar regularmente los medios de respaldo para garantizar que se pueda confiar en ellos para uso de emergencia cuando sea necesario. Probar la capacidad de restaurar datos respaldados en un sistema de prueba, sin sobrescribir los medios de almacenamiento originales en caso de que el proceso de respaldo o restauración falle y cause daños o pérdidas irreparables de datos;

f) proteger las copias de seguridad mediante encriptación de acuerdo con los riesgos identificados (por ejemplo, en situaciones donde la confidencialidad es importante);

g) asegurarse de que se detecte la pérdida inadvertida de datos antes de realizar la copia de seguridad.

Los procedimientos operativos deben monitorear la ejecución de las copias de seguridad y abordar las fallas de las copias de seguridad programadas para garantizar la integridad de las copias de seguridad de acuerdo con la política de copias de seguridad específica del tema.

Las medidas de respaldo para sistemas y servicios individuales deben probarse regularmente para garantizar que cumplan con los objetivos de los planes de respuesta a incidentes y continuidad del negocio (ver5.30). Esto debe combinarse con una prueba de los procedimientos de restauración y compararse con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de sistemas y servicios críticos, las medidas de respaldo deben cubrir toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de un desastre.

Cuando la organización utiliza un servicio en la nube, se deben realizar copias de seguridad de la información, las aplicaciones y los sistemas de la organización en el entorno del servicio en la nube. La organización debe determinar si se cumplen los requisitos de copia de seguridad y de qué manera cuando se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube.

El período de retención de la información comercial esencial debe determinarse, teniendo en cuenta cualquier requisito para la retención de copias de archivo. La organización debe considerar la eliminación de la información (ver8.10) en los medios de almacenamiento utilizados para la copia de seguridad una vez que expire el período de retención de la información y debe tener en cuenta la legislación y las reglamentaciones.

Otra información

Para obtener más información sobre la seguridad del almacenamiento, incluida la consideración de la retención, consulte la norma ISO/IEC 27040.

8.14 Redundancia de las instalaciones de procesamiento de información

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Disponibilidad	# Proteger	# Continuidad # Gestión de activos	# Proteccion # Resiliencia

Control

Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.

Propósito

Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

Guia

La organización debería identificar los requisitos para la disponibilidad de los servicios de negocio y los sistemas de información. La organización debe diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

La redundancia se puede introducir duplicando las instalaciones de procesamiento de información en parte o en su totalidad (es decir, componentes de repuesto o tener dos de todo). La organización debería planificar e implementar procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento. Los procedimientos deben establecer si los componentes redundantes y las actividades de procesamiento son siempre

activada, o en caso de emergencia, automática o manualmente. Los componentes redundantes y las instalaciones de procesamiento de información deben garantizar el mismo nivel de seguridad que los principales.

Deben existir mecanismos para alertar a la organización sobre cualquier falla en las instalaciones de procesamiento de información, permitir la ejecución del procedimiento planificado y permitir la disponibilidad continua mientras se reparan o reemplazan las instalaciones de procesamiento de información.

La organización debe considerar lo siguiente al implementar sistemas redundantes:

a) contratar con dos o más proveedores de redes e instalaciones críticas de procesamiento de información, como proveedores de servicios de Internet;

b) usar redes redundantes;

c) utilizar dos centros de datos separados geográficamente con sistemas duplicados;

d) utilizar fuentes o fuentes de alimentación físicamente redundantes;

e) uso de múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellas (entre instancias en el mismo centro de datos o en diferentes centros de datos);

f) tener componentes duplicados en los sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, cortafuegos, enrutadores, conmutadores).

Cuando corresponda, preferiblemente en modo de producción, los sistemas de información redundantes deben probarse para garantizar que la conmutación por error de un componente a otro funcione según lo previsto.

Otra información

Existe una fuerte relación entre la redundancia y la preparación de las TIC para la continuidad del negocio (ver5.30) especialmente si se requieren tiempos de recuperación cortos. Muchas de las medidas de redundancia pueden formar parte de las estrategias y soluciones de continuidad de las TIC.

La implementación de redundancias puede presentar riesgos para la integridad (p. ej., los procesos de copia de datos en componentes duplicados pueden introducir errores) o la confidencialidad (p. ej., un control de seguridad débil de los componentes duplicados puede comprometer) la información y los sistemas de información, que deben tenerse en cuenta al diseñar sistemas de información.

La redundancia en las instalaciones de procesamiento de información no suele abordar la indisponibilidad de la aplicación debido a fallas dentro de una aplicación.

Con el uso de la computación en la nube pública, es posible tener múltiples versiones en vivo de las instalaciones de procesamiento de información, existentes en múltiples ubicaciones físicas separadas con conmutación por error automática y equilibrio de carga entre ellas.

Algunas de las tecnologías y técnicas para proporcionar redundancia y conmutación por error automática en el contexto de los servicios en la nube se analizan en ISO/IEC TS 23167.

8.15 Registro

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective	# Confidencialidad # Integridad # Disponibilidad	# Detectar	# Information_security_event_management	# Proteccion # Defensa

Control

Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes.

Propósito

Para registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones.

Guia

General

La organización debe determinar el propósito para el cual se crean los registros, qué datos se recopilan y registran y cualquier requisito específico del registro para proteger y manejar los datos de registro. Esto debe documentarse en una política específica del tema sobre el registro.

Los registros de eventos deben incluir para cada evento, si corresponde:

a) identificaciones de usuario;

b) actividades del sistema;

c) fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión);

d) identidad del dispositivo, identificador del sistema y ubicación;

e) direcciones de red y protocolos.

Los siguientes eventos deben ser considerados para el registro:

a) intentos de acceso al sistema exitosos y rechazados;

b) datos exitosos y rechazados y otros intentos de acceso a recursos;

c) cambios en la configuración del sistema;

d) uso de privilegios;

e) uso de programas de utilidad y aplicaciones;

f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

g) alarmas emitidas por el sistema de control de acceso;

h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusos;

i) creación, modificación o supresión de identidades;

j) transacciones ejecutadas por los usuarios en las aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o ejecutado por un tercero.

Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas (ver 8.17) ya que esto permite la correlación de registros entre sistemas para el análisis, alerta e investigación de un incidente.

Protección de registros

Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deben tener permiso para eliminar o desactivar registros de sus propias actividades. Pueden potencialmente manipular los registros en las instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados.

Los controles deben tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro, incluidos:

a) alteraciones en los tipos de mensajes que se registran;

b) archivos de registro que se están editando o eliminando;

c) falla en el registro de eventos o sobreescritura de eventos pasados registrados si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de los registros, se debe considerar el uso de las siguientes técnicas: hashing criptográfico, registro en un archivo de solo lectura y solo para agregar, registro en un archivo de transparencia pública.

Es posible que se requiera archivar algunos registros de auditoría debido a los requisitos sobre la retención de datos o los requisitos para recopilar y conservar evidencia (ver5.28).

Cuando la organización necesite enviar registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o la resolución de errores, los registros deben anonimizarse cuando sea posible utilizando técnicas de enmascaramiento de datos (ver 8.11) para obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlo al proveedor.

Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Deben tomarse las medidas adecuadas de protección de la privacidad (ver5.34).

Análisis de registro

El análisis de registros debe cubrir el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

El análisis de los eventos debe realizarse teniendo en cuenta:

a) las habilidades necesarias para los expertos que realizan el análisis;

b) determinar el procedimiento de análisis de registros;

c) los atributos requeridos de cada evento relacionado con la seguridad;

d) excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, gestión de eventos e información de seguridad (SIEM) o reglas de firewall, y sistemas de detección de intrusos (IDS) o firmas de malware];

e) patrones de comportamiento conocidos y tráfico de red estándar en comparación con actividad y comportamiento anómalos [análisis de comportamiento de usuarios y entidades (UEBA)];

f) resultados del análisis de tendencias o patrones (p. ej., como resultado del uso de análisis de datos, técnicas de macrodatos y herramientas de análisis especializadas);

g) inteligencia de amenazas disponible.

El análisis de registros debe estar respaldado por actividades de monitoreo específicas para ayudar a identificar y analizar el comportamiento anómalo, que incluye:

a) revisar los intentos exitosos y fallidos de acceder a los recursos protegidos [por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y recursos compartidos de archivos];

b) verificar los registros de DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados con servidores de comando y control de botnet;

c) examinar los informes de uso de los proveedores de servicios (p. ej., facturas o informes de servicios) en busca de actividad inusual dentro de los sistemas y redes (p. ej., mediante la revisión de patrones de actividad);

d) incluir registros de eventos de monitoreo físico, como entrada y salida, para garantizar una detección y un análisis de incidentes más precisos;

e) correlación de registros para permitir un análisis eficiente y altamente preciso.

Los incidentes de seguridad de la información presuntos y reales deben identificarse (p. ej., infección de malware o sondeo de cortafuegos) y estar sujetos a una mayor investigación (p. ej., como parte de un proceso de gestión de incidentes de seguridad de la información, consulte5.25).

Otra información

Los registros del sistema suelen contener un gran volumen de información, gran parte de la cual es ajena al control de la seguridad de la información. Para ayudar a identificar eventos significativos con fines de monitoreo de la seguridad de la información, se puede considerar el uso de programas de utilidad o herramientas de auditoría adecuados para realizar la interrogación de archivos.

El registro de eventos sienta las bases para los sistemas de monitoreo automatizados (ver8.16) que son capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

Se puede utilizar una herramienta SIEM o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro., y generar alertas. Los SIEM tienden a requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones a considerar incluyen la identificación y selección de fuentes de registro apropiadas, ajuste y prueba de reglas y desarrollo de casos de uso.

Los archivos de transparencia pública para el registro de registros se utilizan, por ejemplo, en sistemas de transparencia de certificados. Dichos archivos pueden proporcionar un mecanismo de detección adicional útil para protegerse contra la manipulación del registro.

En entornos de nube, las responsabilidades de gestión de registros se pueden compartir entre el cliente del servicio de nube y el proveedor de servicios de nube. Las responsabilidades varían según el tipo de servicio en la nube que se utilice. Puede encontrar más orientación en ISO / IEC 27017.

8.16 Actividades de seguimiento

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective # Correctivo	# Confidencialidad # Integridad #Disponibilidad	# Detectar #Responder	# Information_security_event_management	# Defensa

Control

Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Guia

El alcance y el nivel de monitoreo deben determinarse de acuerdo con los requisitos de seguridad de la información y del negocio y teniendo en cuenta las leyes y regulaciones pertinentes. Los registros de seguimiento deben mantenerse durante períodos de retención definidos.

Lo siguiente debe ser considerado para su inclusión dentro del sistema de monitoreo:

a) tráfico de red, sistema y aplicación entrante y saliente;

b) acceso a sistemas, servidores, equipos de red, sistema de monitoreo, aplicaciones críticas, etc.;

c) archivos de configuración de red y sistema de nivel crítico o administrativo;

d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos];

e) registros de eventos relacionados con la actividad del sistema y de la red;

f) comprobar que el código que se ejecuta está autorizado para ejecutarse en el sistema y que no ha sido alterado (p. ej., mediante recompilación para agregar código adicional no deseado);

g) uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

La organización debe establecer una línea de base de comportamiento normal y monitorear contra esta línea de base para detectar anomalías. Al establecer una línea de base, se debe considerar lo siguiente:

a) revisar la utilización de los sistemas en períodos normales y pico;

b) hora habitual de acceso, lugar de acceso, frecuencia de acceso para cada usuario o grupo de usuarios.

El sistema de monitoreo debe configurarse contra la línea de base establecida para identificar comportamientos anómalos, tales como:

a) terminación no planificada de procesos o aplicaciones;

b) actividad típicamente asociada con malware o tráfico que se origina en direcciones IP o dominios de red maliciosos conocidos (por ejemplo, aquellos asociados con servidores de comando y control de botnet);

c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamiento de memoria intermedia);

d) comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar);

e) cuellos de botella y sobrecargas (por ejemplo, colas de la red, niveles de latencia y fluctuaciones de la red);

f) acceso no autorizado (real o intentado) a sistemas o información;

g) escaneo no autorizado de aplicaciones comerciales, sistemas y redes;

h) intentos exitosos y fallidos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos);

i) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

Se debe utilizar un monitoreo continuo a través de una herramienta de monitoreo. El monitoreo debe hacerse en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la organización. Las herramientas de monitoreo deben incluir la capacidad de manejar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también deberían poder reconocer firmas y datos específicos o patrones de comportamiento de la red o la aplicación.

El software de monitoreo automatizado debe configurarse para generar alertas (por ejemplo, a través de consolas de administración, mensajes de correo electrónico o sistemas de mensajería instantánea) en función de umbrales predefinidos. El sistema de alerta debe ajustarse y capacitarse en la línea de base de la organización para minimizar los falsos positivos. El personal debe dedicarse a responder a las alertas y debe estar debidamente capacitado para interpretar con precisión los posibles incidentes. Debe haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los eventos anormales deben comunicarse a las partes relevantes para mejorar las siguientes actividades: auditoría, evaluación de seguridad, exploración y monitoreo de vulnerabilidades (ver5.25). Deben existir procedimientos para responder a los indicadores positivos del sistema de monitoreo de manera oportuna, a fin de minimizar el efecto de los eventos adversos (ver5.26) sobre seguridad de la información. También se deben establecer procedimientos para identificar y abordar los falsos positivos, incluido el ajuste del software de monitoreo para reducir la cantidad de falsos positivos en el futuro.

Otra información

El monitoreo de la seguridad se puede mejorar mediante:

a) aprovechar los sistemas de inteligencia de amenazas (ver5.7);

b) aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) usar listas de bloqueo o listas de permitidos;

d) realizar una variedad de evaluaciones técnicas de seguridad (p. ej., evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ataques cibernéticos y ejercicios de respuesta cibernética) y usar los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;

e) usar sistemas de monitoreo del desempeño para ayudar a establecer y detectar comportamientos anómalos;

f) aprovechamiento de registros en combinación con sistemas de seguimiento.

Las actividades de monitoreo a menudo se realizan utilizando software especializado, como los sistemas de detección de intrusos. Estos se pueden configurar a una línea de base de actividades normales, aceptables y esperadas del sistema y de la red.

El monitoreo de comunicaciones anómalas ayuda en la identificación de botnets (es decir, un conjunto de dispositivos bajo el control malicioso del propietario de la botnet, generalmente utilizados para montar ataques distribuidos de denegación de servicio en otras computadoras de otras organizaciones). Si la computadora está siendo controlada por un dispositivo externo, existe una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, la organización debe emplear tecnologías para monitorear comunicaciones anómalas y tomar las medidas necesarias.

8.17 Sincronización del reloj

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Detective	# Integridad	# Proteger #Detectar	# Information_security_event_management	# Proteccion # Defensa

Control

Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.

Propósito

Permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y respaldar las investigaciones sobre incidentes de seguridad de la información.

Guia

Los requisitos externos e internos para la representación del tiempo, la sincronización confiable y la precisión deben documentarse e implementarse. Dichos requisitos pueden provenir de necesidades legales, estatutarias, reglamentarias, contractuales, estándares y de control interno. Se debe definir y considerar un tiempo de referencia estándar para uso dentro de la organización para todos los sistemas, incluidos los sistemas de administración de edificios, los sistemas de entrada y salida y otros que se pueden usar para ayudar en las investigaciones.

Un reloj vinculado a una transmisión de tiempo por radio desde un reloj atómico nacional o un sistema de posicionamiento global (GPS) debe usarse como reloj de referencia para los sistemas de registro; una fuente de fecha y hora consistente y confiable para garantizar sellos de tiempo precisos. Deben utilizarse protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) para mantener todos los sistemas en red sincronizados con un reloj de referencia.

La organización puede usar dos fuentes de tiempo externas al mismo tiempo para mejorar la confiabilidad de los relojes externos y administrar adecuadamente cualquier variación.

La sincronización del reloj puede ser difícil cuando se usan múltiples servicios en la nube o cuando se usan tanto servicios en la nube como locales. En este caso, se debe monitorear el reloj de cada servicio y registrar la diferencia para mitigar los riesgos derivados de las discrepancias.

Otra información

La configuración correcta de los relojes de las computadoras es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden dificultar dichas investigaciones y dañar la credibilidad de dicha evidencia.

8.18 Uso de programas de utilidad privilegiados

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# sistema_y_red-trabajo_seguridad # Secure_configura-ción #Aplicación_seguridad	# Proteccion

Control

El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones debe restringirse y controlarse estrictamente.

Propósito

Para garantizar que el uso de programas de utilidad no dañe el sistema y los controles de aplicaciones para la seguridad de la información.

Guia

Se deben considerar las siguientes pautas para el uso de programas de utilidad que pueden anular los controles del sistema y de la aplicación:

a) limitación del uso de programas de utilidad al número mínimo práctico de usuarios autorizados de confianza (ver8.2);

b) uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluida la identificación única de la persona que usa el programa de utilidad;

c) definir y documentar los niveles de autorización para los programas de servicios públicos;

d) autorización para uso ad hoc de programas utilitarios;

e) no poner programas de utilidad a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere segregación de funciones;

f) eliminar o deshabilitar todos los programas de utilidad innecesarios;

g) como mínimo, separación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para tales programas del tráfico de aplicaciones;

h) limitación de la disponibilidad de los programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todos los usos de los programas de utilidad.

Otra información

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

8.19 Instalación de software en sistemas operativos

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# configuración_segura #Aplicación_seguridad	# Proteccion

Control

Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

Propósito

Para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

Guia

Se deben considerar las siguientes pautas para administrar de forma segura los cambios y la instalación de software en los sistemas operativos:

a) realizar actualizaciones del software operativo solo por parte de administradores capacitados con la autorización de gestión adecuada (ver8.5);

b) garantizar que solo se instale código ejecutable aprobado y ningún código de desarrollo o compiladores en los sistemas operativos;

c) solo instalar y actualizar el software después de pruebas extensas y exitosas (ver8.29 y8.31);

d) actualizar todas las bibliotecas fuente de programas correspondientes;

e) usar un sistema de control de configuración para mantener el control de todo el software operativo, así como la documentación del sistema;

f) definir una estrategia de reversión antes de que se implementen los cambios;

g) mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) archivar versiones antiguas de software, junto con toda la información y parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia, y durante el tiempo que se requiera que el software lea o procese datos archivados.

Cualquier decisión de actualizar a una nueva versión debe tener en cuenta los requisitos comerciales para el cambio y la seguridad de la versión (p. ej., la introducción de una nueva funcionalidad de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual). Los parches de software deben aplicarse cuando puedan ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información (ver8.8 y 8.19).

El software de computadora puede basarse en software y paquetes suministrados externamente (por ejemplo, programas de software que utilizan módulos alojados en sitios externos), que deben monitorearse y controlarse para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades de seguridad de la información.

El software suministrado por el proveedor que se utiliza en los sistemas operativos debe mantenerse en un nivel respaldado por el proveedor. Con el tiempo, los proveedores de software dejarán de admitir versiones anteriores de software. La organización debe considerar los riesgos de depender de software sin soporte. El software de código abierto utilizado en los sistemas operativos debe mantenerse hasta la última versión adecuada del software. Con el tiempo, el código fuente abierto puede dejar de mantenerse, pero aún está disponible en un repositorio de software de código abierto. La organización también debe considerar los riesgos de confiar en software de código abierto sin mantenimiento cuando se usa en sistemas operativos.

Cuando los proveedores estén involucrados en la instalación o actualización de software, el acceso físico o lógico solo debe otorgarse cuando sea necesario y con la debida autorización. Las actividades del proveedor deben ser monitoreadas (ver5.22).

La organización debe definir y hacer cumplir reglas estrictas sobre qué tipos de software pueden instalar los usuarios.

El principio de privilegio mínimo debe aplicarse a la instalación de software en sistemas operativos. La organización debe identificar qué tipos de instalaciones de software están permitidas (p. ej., actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (p. ej., software que es solo para uso personal y software cuyo pedigrí con respecto a ser potencialmente malicioso se desconoce o sospechar). Estos privilegios deben otorgarse en función de las funciones de los usuarios en cuestión.

Otra información

Ninguna otra información.

8.20 Seguridad de redes

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Proteger #Detectar	# sistema_y_red-trabajo_seguridad	# Proteccion

Control

Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en los sistemas y aplicaciones.

Propósito

Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.

Guia

Se deben implementar controles para garantizar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado. En particular, se deben considerar los siguientes elementos:

a) el tipo y nivel de clasificación de la información que la red puede soportar;

b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores);

d) separar la responsabilidad operativa de las redes de las operaciones del sistema TIC cuando corresponda (ver5.3);

e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger los sistemas y aplicaciones conectados (ver5.22 ,8.24 ,5.14 y6.6). También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y las computadoras conectadas a la red;

f) registro y monitoreo adecuados para permitir el registro y la detección de acciones que pueden afectar o son relevantes para la seguridad de la información (ver8.16 y8.15);

g) coordinar estrechamente las actividades de gestión de la red tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de forma coherente en toda la infraestructura de procesamiento de la información;

h) sistemas de autenticación en la red;

i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, usando firewalls);

j) detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) endurecimiento de los dispositivos de red;

l) segregar los canales de administración de red de otro tráfico de red;

m) aislar temporalmente subredes críticas (por ejemplo, con puentes levadizos) si la red está bajo ataque;

n) deshabilitar protocolos de red vulnerables.

La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas. Las redes virtualizadas también cubren las redes definidas por software (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la separación lógica de la comunicación que tiene lugar en las redes físicas, en particular para los sistemas y aplicaciones que se implementan mediante computación distribuida.

Otra información

Puede encontrar información adicional sobre la seguridad de la red en la serie ISO/IEC 27033.

Se puede encontrar más información sobre redes virtualizadas en ISO / IEC TS 23167.

8.21 Seguridad de los servicios de red

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# sistema_y_red- trabajo_seguridad	# Proteccion

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben identificarse, implementarse y monitorearse.

Propósito

Para garantizar la seguridad en el uso de los servicios de red.

Guia

Las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio, deben ser identificadas e implementadas (por proveedores de servicios de red internos o externos). La organización debe asegurarse de que los proveedores de servicios de red implementen estas medidas.

La capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura debe determinarse y controlarse periódicamente. El derecho a la auditoría debe acordarse entre la organización y el proveedor. La organización también debe considerar las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Las reglas sobre el uso de redes y servicios de red deben formularse e implementarse para cubrir:

a) las redes y los servicios de red a los que se permite acceder;

b) requisitos de autenticación para acceder a diversos servicios de red;

c) procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;

d) administración de redes y controles tecnológicos y procedimientos para proteger el acceso a conexiones de red y servicios de red;

e) los medios utilizados para acceder a redes y servicios de red [por ejemplo, uso de red privada virtual (VPN) o red inalámbrica];

f) hora, ubicación y otros atributos del usuario al momento del acceso;

g) seguimiento del uso de los servicios de red.

Se deben considerar las siguientes características de seguridad de los servicios de red:

a) tecnología aplicada para la seguridad de los servicios de red, como autenticación, encriptación y controles de conexión a la red;

b) parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las normas de seguridad y conexión a la red;

c) almacenamiento en caché (por ejemplo, en una red de entrega de contenido) y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad;

d) procedimientos para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

Otra información

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos. Estos servicios pueden variar desde ancho de banda simple no administrado hasta ofertas complejas de valor agregado.

En ISO / IEC 29146 se proporciona más orientación sobre un marco para la gestión de acceso.

8.22 Segregación de redes

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# sistema_y_red-trabajo_seguridad	# Proteccion

Control

Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

Propósito

Para dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales.

Guia

La organización debería considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet). Los dominios se pueden elegir en función de los niveles de confianza, criticidad y sensibilidad (p. ej., dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de alto y bajo riesgo), junto con unidades organizativas (p. ej., recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio del servidor que se conecta a varias unidades organizativas). La segregación se puede realizar usando redes físicamente diferentes o usando diferentes redes lógicas.

El perímetro de cada dominio debe estar bien definido. Si se permite el acceso entre dominios de red, debe controlarse en el perímetro mediante una puerta de enlace (por ejemplo, cortafuegos, enrutador de filtrado). Los criterios para

la segregación de redes en dominios y el acceso permitido a través de las puertas de enlace deben basarse en una evaluación de los requisitos de seguridad de cada dominio. La evaluación debe estar de acuerdo con la política específica del tema sobre el control de acceso (ver5.15), los requisitos de acceso, el valor y la clasificación de la información procesada y tener en cuenta el coste relativo y el impacto en el rendimiento de la incorporación de una tecnología de puerta de enlace adecuada.

Las redes inalámbricas requieren un tratamiento especial debido al perímetro de red mal definido. Se debe considerar el ajuste de la cobertura de radio para la segregación de redes inalámbricas. Para entornos sensibles, se debe considerar tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de las redes internas hasta que el acceso haya pasado a través de una puerta de enlace de acuerdo con los controles de la red (ver8.20) antes de otorgar acceso a los sistemas internos. La red de acceso inalámbrico para invitados debe separarse de las del personal si el personal solo usa dispositivos de punto final de usuario controlados que cumplen con las políticas específicas del tema de la organización. El WiFi para invitados debe tener al menos las mismas restricciones que el WiFi para el personal, a fin de desalentar el uso del WiFi de invitados por parte del personal.

Otra información

Las redes a menudo se extienden más allá de los límites organizacionales, ya que se forman asociaciones comerciales que requieren la interconexión o el intercambio de instalaciones de redes y procesamiento de información. Dichas extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que usan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

8.23 Filtrado web

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# sistema_y_red-trabajo_seguridad	# Proteccion

Control

El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.

Propósito

Para proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.

Guia

La organización debe reducir los riesgos de que su personal acceda a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing. Una técnica para lograr esto funciona bloqueando la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware hacen esto automáticamente o pueden configurarse para hacerlo.

La organización debe identificar los tipos de sitios web a los que el personal debe o no tener acceso. La organización debería considerar bloquear el acceso a los siguientes tipos de sitios web:

a) sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas;

b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing);

c) servidores de mando y control;

d) sitio web malicioso adquirido de inteligencia de amenazas (ver5.7);

e) sitios web que comparten contenido ilegal.

Antes de implementar este control, la organización debe establecer reglas para el uso seguro y apropiado de los recursos en línea, incluida cualquier restricción a sitios web y aplicaciones basadas en la web indeseables o inapropiados. Las reglas deben mantenerse actualizadas.

Se debe capacitar al personal sobre el uso seguro y apropiado de los recursos en línea, incluido el acceso a la web. La capacitación debe incluir las reglas de la organización, el punto de contacto para plantear problemas de seguridad y el proceso de excepción cuando se necesita acceder a recursos web restringidos por razones comerciales legítimas. También se debe capacitar al personal para asegurarse de que no invalide ningún aviso del navegador que informe que un sitio web no es seguro pero permite que el usuario continúe.

Otra información

El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que el software malicioso y otras actividades maliciosas ataquen la red y los sistemas de la organización.

8.24 Uso de criptografía

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# configuración_segura	# Proteccion

Control

Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Propósito

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Guia

General

Al usar criptografía, se debe considerar lo siguiente:

a) la política específica del tema sobre criptografía definida por la organización, incluidos los principios generales para la protección de la información. Es necesaria una política específica sobre el uso de la criptografía para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y para evitar el uso inapropiado o incorrecto;

b) identificar el nivel de protección requerido y la clasificación de la información y en consecuencia establecer el tipo, fortaleza y calidad de los algoritmos criptográficos requeridos;

c) el uso de criptografía para la protección de la información contenida en los dispositivos móviles o medios de almacenamiento de los usuarios y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;

d) el enfoque de la gestión de claves, incluidos los métodos para gestionar la generación y protección de claves criptográficas y la recuperación de información cifrada en caso de pérdida, compromiso o daño de claves;

e) roles y responsabilidades para:

1) la implementación de las reglas para el uso efectivo de la criptografía;

2) la gestión de claves, incluida la generación de claves (ver8.24);

f) los estándares a adoptar, así como los algoritmos criptográficos, la fuerza del cifrado, las soluciones criptográficas y las prácticas de uso que se aprueban o requieren para su uso en la organización;

g) el impacto del uso de información cifrada en los controles que se basan en la inspección de contenido (por ejemplo, detección de malware o filtrado de contenido).

Al implementar las reglas de la organización para el uso eficaz de la criptografía, se deben tener en cuenta las reglamentaciones y las restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas en diferentes partes del mundo, así como los problemas del flujo transfronterizo de información cifrada (mar 5.31).

El contenido de los acuerdos o contratos de nivel de servicio con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) debe cubrir cuestiones de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la prestación de servicios (ver5.22).

Gestión de claves

La gestión adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Un sistema de gestión de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) emitir y obtener certificados de clave pública;

c) distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben;

d) claves de almacenamiento, incluida la forma en que los usuarios autorizados obtienen acceso a las claves;

e) cambiar o actualizar las claves, incluidas las reglas sobre cuándo cambiar las claves y cómo se hará;

f) tratar con claves comprometidas;

g) revocación de claves, incluido cómo retirar o desactivar claves [por ejemplo, cuando las claves se han visto comprometidas o cuando un usuario abandona una organización (en cuyo caso, las claves también deben archivarse)];

h) recuperar claves perdidas o dañadas;

i) realizar copias de seguridad o archivar claves;

j) destrucción de llaves;

k) registro y auditoría de actividades clave relacionadas con la gestión;

l) establecer las fechas de activación y desactivación de las claves para que las claves solo se puedan usar durante el período de tiempo de acuerdo con las reglas de la organización sobre administración de claves;

m) tramitar solicitudes legales de acceso a claves criptográficas (p. ej., se puede exigir que la información cifrada esté disponible sin cifrar como prueba en un caso judicial).

Todas las claves criptográficas deben protegerse contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado y la divulgación. El equipo utilizado para generar, almacenar y archivar claves debe protegerse físicamente.

Además de la integridad, para muchos casos de uso, también se debe considerar la autenticidad de las claves públicas.

Otra información

La autenticidad de las claves públicas generalmente se aborda mediante procesos de administración de claves públicas que utilizan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante el uso de tecnologías como la aplicación de procesos manuales para claves de números pequeños.

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: uso de cifrado de información para proteger información sensible o crítica, ya sea almacenada o transmitida;

b) integridad o autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Usar algoritmos con el fin de verificar la integridad de los archivos;

c) no repudio: uso de técnicas criptográficas para proporcionar evidencia de la ocurrencia o no ocurrencia de un evento o acción;

d) autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso o realizan transacciones con usuarios, entidades y recursos del sistema.

La serie ISO/IEC 11770 proporciona más información sobre la gestión de claves.

8.25 Ciclo de vida de desarrollo seguro

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red-trabajo_seguridad	# Proteccion

Control

Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

Propósito

Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.

Guia

El desarrollo seguro es un requisito para crear un servicio, una arquitectura, un software y un sistema seguros. Para lograrlo, se deben considerar los siguientes aspectos:

a) separación de los entornos de desarrollo, prueba y producción (ver8.31);

b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software:

1) seguridad en la metodología de desarrollo de software (ver8.28 y8.27);

2) pautas de codificación segura para cada lenguaje de programación utilizado (ver8.28);

c) requisitos de seguridad en la fase de especificación y diseño (ver5.8);

d) puntos de control de seguridad en proyectos (ver5.8);

e) pruebas de sistema y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración (ver8.29);

f) repositorios seguros para el código fuente y la configuración (ver8.4 y8.9);

g) seguridad en el control de versiones (ver8.32);

h) conocimiento y capacitación en seguridad de la aplicación requeridos (ver8.28);

i) la capacidad de los desarrolladores para prevenir, encontrar y reparar vulnerabilidades (ver8.28);

j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (ver5.32).

Si se subcontrata el desarrollo, la organización debe asegurarse de que el proveedor cumpla con las reglas de la organización para el desarrollo seguro (ver8.30).

Otra información

El desarrollo también puede tener lugar dentro de aplicaciones, como aplicaciones de oficina, secuencias de comandos, navegadores y bases de datos.

8.26 Requisitos de seguridad de la aplicación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red-trabajo_seguridad	# Proteccion # Defensa

Control

Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

Propósito

Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

Guia

General

Deben identificarse y especificarse los requisitos de seguridad de las aplicaciones. Estos requisitos generalmente se determinan a través de una evaluación de riesgos. Los requisitos deben desarrollarse con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de la aplicación pueden cubrir una amplia gama de temas, según el propósito de la aplicación.

Los requisitos de seguridad de la aplicación deben incluir, si corresponde:

a) nivel de confianza en la identidad de las entidades [por ejemplo, a través de la autenticación (ver5.17 ,8.2 y8.5)];

b) identificar el tipo de información y el nivel de clasificación a ser procesado por la aplicación;

c) necesidad de segregación de acceso y nivel de acceso a datos y funciones en la aplicación;

d) resiliencia contra ataques maliciosos o interrupciones no intencionales [por ejemplo, protección contra desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL)];

e) requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción;

f) necesidad de privacidad asociada con todas las partes involucradas;

g) los requisitos de protección de cualquier información confidencial;

h) protección de datos en proceso, en tránsito y en reposo;

i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas;

j) controles de entrada, incluidas verificaciones de integridad y validación de entrada;

k) controles automatizados (por ejemplo, límites de aprobación o aprobaciones dobles);

l) controles de salida, considerando también quién puede acceder a las salidas y su autorización;

m) restricciones en torno al contenido de los campos de "texto libre", ya que pueden conducir al almacenamiento incontrolado de datos confidenciales (por ejemplo, datos personales);

n) requisitos derivados del proceso de negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio;

o) requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para registro y monitoreo o sistemas de detección de fuga de datos);

p) manejo de mensajes de error.

Servicios transaccionales

Además, para las aplicaciones que ofrecen servicios transaccionales entre la organización y un socio, se debe considerar lo siguiente al identificar los requisitos de seguridad de la información:

a) el nivel de confianza que cada parte requiere en la identidad reclamada de la otra parte;

b) el nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para la identificación de la falta de integridad (por ejemplo, verificación de redundancia cíclica, hashing, firmas digitales);

c) procesos de autorización asociados con quién puede aprobar contenidos, emitir o firmar documentos transaccionales clave;

d) confidencialidad, integridad, prueba de envío y recepción de documentos clave y no repudio (por ejemplo, contratos asociados a procesos de licitación y contratación);

e) la confidencialidad e integridad de cualquier transacción (por ejemplo, pedidos, detalles de la dirección de entrega y confirmación de recibos);

f) requisitos sobre cuánto tiempo mantener una transacción confidencial;

g) seguros y otros requisitos contractuales.

Aplicaciones de pago y pedidos electrónicos

Además, para aplicaciones que involucren pedidos y pagos electrónicos, se debe considerar lo siguiente:

a) requisitos para mantener la confidencialidad e integridad de la información de la orden;

b) el grado de verificación apropiado para verificar la información de pago proporcionada por un cliente;

c) evitar la pérdida o duplicación de información de transacciones;

d) almacenar los detalles de la transacción fuera de cualquier entorno de acceso público (p. ej., en una plataforma de almacenamiento existente en la intranet de la organización, y no retenida ni expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet);

e) cuando se utiliza una autoridad de confianza (p. ej., con el fin de emitir y mantener firmas digitales o certificados digitales), la seguridad se integra y se incorpora a lo largo de todo el proceso de gestión de firmas o certificados de extremo a extremo.

Varias de las consideraciones anteriores pueden abordarse mediante la aplicación de la criptografía (ver8.24), teniendo en cuenta los requisitos legales (ver5.31 para5.36 , especialmente ver5.31 para la legislación criptográfica).

Otra información

Las aplicaciones accesibles a través de las redes están sujetas a una variedad de amenazas relacionadas con la red, como actividades fraudulentas, disputas de contratos o divulgación de información al público; transmisión incompleta, enrutamiento erróneo, alteración no autorizada de mensajes, duplicación o reproducción. Por lo tanto, las evaluaciones de riesgo detalladas y la determinación cuidadosa de los controles son indispensables. Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y la seguridad de la transferencia de datos.

Puede encontrar más información sobre la seguridad de las aplicaciones en la serie ISO/IEC 27034.

8.27 Arquitectura del sistema seguro y principios de ingeniería

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red- trabajo_seguridad	# Proteccion

Control

Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

Guia

Los principios de ingeniería de seguridad deben establecerse, documentarse y aplicarse a las actividades de ingeniería de sistemas de información. La seguridad debe diseñarse en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología). La nueva tecnología debe analizarse en busca de riesgos de seguridad y el diseño debe revisarse frente a patrones de ataque conocidos.

Los principios de ingeniería segura brindan orientación sobre técnicas de autenticación de usuarios, control de sesión seguro y validación y saneamiento de datos.

Los principios de ingeniería de sistemas seguros deben incluir el análisis de:

a) la gama completa de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas;

b) las capacidades de los controles de seguridad para prevenir, detectar o responder a eventos de seguridad;

c) controles de seguridad específicos requeridos por procesos comerciales particulares (por ejemplo, encriptación de información confidencial, verificación de integridad y firma digital de información);

d) dónde y cómo se aplicarán los controles de seguridad (p. ej., mediante la integración con una arquitectura de seguridad y la infraestructura técnica);

e) cómo los controles de seguridad individuales (manuales y automatizados) funcionan juntos para producir un conjunto integrado de controles.

Los principios de ingeniería de seguridad deberían tener en cuenta:

a) la necesidad de integrarse con una arquitectura de seguridad;

b) infraestructura de seguridad técnica [por ejemplo, infraestructura de clave pública (PKI), gestión de acceso e identidad (IAM), prevención de fuga de datos y gestión de acceso dinámico];

c) capacidad de la organización para desarrollar y soportar la tecnología elegida;

d) costo, tiempo y complejidad de cumplir con los requisitos de seguridad;

e) buenas prácticas actuales.

La ingeniería de sistemas seguros debe implicar:

a) el uso de principios de arquitectura de seguridad, tales como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación predeterminada", "fallo seguro", "desconfianza de la entrada de aplicaciones externas", "seguridad en implementación", "asumir incumplimiento", "privilegio mínimo", "usabilidad y manejabilidad" y "funcionalidad mínima";

b) una revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de la seguridad de la información, asegurar que se especifiquen los controles de seguridad y cumplir con los requisitos de seguridad;

c) documentación y reconocimiento formal de los controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad superiores);

d) endurecimiento de los sistemas.

La organización debe considerar principios de "confianza cero" tales como:

a) suponiendo que los sistemas de información de la organización ya están violados y, por lo tanto, no dependen solo de la seguridad del perímetro de la red;

b) emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información;

c) garantizar que las solicitudes a los sistemas de información estén encriptadas de extremo a extremo;

d) verificar cada solicitud a un sistema de información como si se originara en una red externa abierta, incluso si estas solicitudes se originaron internamente en la organización (es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros);

e) usar técnicas de control de acceso dinámico y de "privilegio mínimo" (ver5.15 ,5.18 y8.2). Esto incluye autenticar y autorizar solicitudes de información o a sistemas basados en información contextual, como información de autenticación (ver5.17), identidades de usuario (ver5.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (ver5.12);

f) siempre autenticando a los solicitantes y siempre validando las solicitudes de autorización a los sistemas de información en base a la información, incluida la información de autenticación (ver5.17) e identidades de usuario (5.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (ver5.12), por ejemplo, hacer cumplir una autenticación sólida (p. ej., multifactor, consulte8.5).

Los principios de ingeniería de seguridad establecidos deben aplicarse, cuando corresponda, al desarrollo subcontratado de sistemas de información a través de contratos y otros acuerdos vinculantes entre la organización y el proveedor a quien la organización subcontrata. La organización debe garantizar que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la organización.

Los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos deben revisarse periódicamente para garantizar que contribuyan efectivamente a mejorar los estándares de seguridad dentro del proceso de ingeniería. También deben revisarse periódicamente para garantizar que permanezcan actualizados en términos de combatir cualquier nueva amenaza potencial y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Otra información

Los principios de ingeniería segura se pueden aplicar al diseño o configuración de una variedad de técnicas, como:

- tolerancia a fallas y otras técnicas de resiliencia;

- segregación (por ejemplo, mediante virtualización o contenedorización);

- resistencia a la manipulación.

Se pueden utilizar técnicas de virtualización seguras para evitar la interferencia entre aplicaciones que se ejecutan en el mismo dispositivo físico. Si un atacante pone en peligro una instancia virtual de una aplicación, solo esa instancia se ve afectada. El ataque no tiene efecto en ninguna otra aplicación o datos.

Las técnicas de resistencia a la manipulación pueden utilizarse para detectar la manipulación de contenedores de información, ya sea física (p. ej., una alarma antirrobo) o lógica (p. ej., un archivo de datos). Una característica de tales técnicas es que existe un registro del intento de manipulación del contenedor. Además, el control puede impedir la correcta extracción de datos mediante su destrucción (p. ej., se puede borrar la memoria del dispositivo).

8.28 Codificación segura

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Seguridad do- red eléctrica
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # Sistema_y_red_ seguridad	# Proteccion

Control

Los principios de codificación segura deben aplicarse al desarrollo de software.

Propósito

Garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.

Guia

General

La organización debe establecer procesos en toda la organización para proporcionar una buena gobernanza para la codificación segura. Se debe establecer y aplicar una línea de base segura mínima. Además, dichos procesos y gobernanza deben extenderse para cubrir los componentes de software de terceros y el software de código abierto.

La organización debe monitorear las amenazas del mundo real y actualizar el asesoramiento y la información sobre las vulnerabilidades del software para guiar los principios de codificación segura de la organización a través de la mejora y el aprendizaje continuos. Esto puede ayudar a garantizar que se implementen prácticas de codificación seguras y efectivas para combatir el panorama de amenazas que cambia rápidamente.

Planificación y antes de codificar

Los principios de codificación segura deben usarse tanto para nuevos desarrollos como en escenarios de reutilización. Estos principios deben aplicarse a las actividades de desarrollo tanto dentro de la organización como para los productos y servicios que la organización proporciona a otros. La planificación y los requisitos previos antes de la codificación deben incluir:

a) expectativas específicas de la organización y principios aprobados para la codificación segura que se utilizará para desarrollos de código internos y externos;

b) prácticas y defectos de codificación comunes e históricos que conducen a vulnerabilidades de seguridad de la información;

c) configurar herramientas de desarrollo, como entornos de desarrollo integrados (IDE), para ayudar a hacer cumplir la creación de código seguro;

d) seguir la orientación emitida por los proveedores de herramientas de desarrollo y entornos de ejecución, según corresponda;

e) mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores);

f) calificación de los desarrolladores en la escritura de código seguro;

g) diseño y arquitectura seguros, incluido el modelado de amenazas;

h) normas de codificación seguras y, cuando corresponda, exigir su uso;

i) uso de ambientes controlados para el desarrollo.

Durante la codificación

Las consideraciones durante la codificación deben incluir:

a) prácticas de codificación seguras específicas para los lenguajes de programación y técnicas que se utilizan;

b) utilizar técnicas de programación seguras, como programación en pares, refactorización, revisión por pares, iteraciones de seguridad y desarrollo basado en pruebas;

c) utilizando técnicas de programación estructurada;

d) documentar el código y eliminar los defectos de programación, lo que puede permitir que se exploten las vulnerabilidades de seguridad de la información;

e) prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, ejemplos de código no aprobados y servicios web no autenticados).

Las pruebas deben realizarse durante y después del desarrollo (ver8.29). Los procesos de prueba de seguridad de aplicaciones estáticas (SAST) pueden identificar vulnerabilidades de seguridad en el software.

Antes de que el software entre en funcionamiento, se debe evaluar lo siguiente:

a) superficie de ataque y el principio de privilegio mínimo;

b) realizar un análisis de los errores de programación más comunes y documentar que estos han sido mitigados.

Revisión y mantenimiento

Después de que el código se haya hecho operativo:

a) las actualizaciones deben empaquetarse e implementarse de forma segura;

b) se deben manejar las vulnerabilidades de seguridad de la información informadas (ver8.8);

c) los errores y los ataques sospechosos deben registrarse y los registros deben revisarse periódicamente para hacer los ajustes necesarios al código;

d) el código fuente debe protegerse contra el acceso no autorizado y la manipulación (p. ej., mediante el uso de herramientas de gestión de la configuración, que suelen proporcionar funciones como control de acceso y control de versiones).

Si utiliza herramientas y bibliotecas externas, la organización debe considerar:

a) garantizar que las bibliotecas externas se gestionen (p. ej., manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualicen periódicamente con los ciclos de publicación;

b) selección, autorización y reutilización de componentes bien examinados, en particular componentes de autenticación y criptográficos;

c) la licencia, seguridad e historial de los componentes externos;

d) garantizar que el software se pueda mantener, rastrear y provenir de fuentes comprobadas y confiables;

e) disponibilidad a largo plazo de recursos y artefactos para el desarrollo.

Cuando sea necesario modificar un paquete de software, se deben considerar los siguientes puntos:

a) el riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos;

b) si se debe obtener el consentimiento del vendedor;

c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar del programa;

d) el impacto si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios;

e) compatibilidad con otro software en uso.

Otra información

Un principio rector es garantizar que el código relevante para la seguridad se invoque cuando sea necesario y sea resistente a la manipulación. Los programas instalados a partir de código binario compilado también tienen estas propiedades, pero solo para los datos contenidos en la aplicación. Para los lenguajes interpretados, el concepto solo funciona cuando el código se ejecuta en un servidor que, de otro modo, es inaccesible para los usuarios y los procesos que lo usan, y que sus datos se mantienen en una base de datos protegida de manera similar. Por ejemplo, el código interpretado se puede ejecutar en un servicio en la nube donde el acceso al código requiere privilegios de administrador. Dicho acceso de administrador debe estar protegido por mecanismos de seguridad, como los principios de administración justo a tiempo y la autenticación fuerte. Si el propietario de la aplicación puede acceder a los scripts mediante acceso remoto directo al servidor, en principio también puede hacerlo un atacante.

El código de la aplicación se diseña mejor asumiendo que siempre está sujeto a ataques, por error o acción maliciosa. Además, las aplicaciones críticas pueden diseñarse para ser tolerantes a fallas internas. Por ejemplo, la salida de un algoritmo complejo puede verificarse para asegurarse de que se encuentra dentro de límites seguros antes de que los datos se utilicen en una aplicación como una aplicación financiera o de seguridad crítica. El código que realiza las comprobaciones de límites es simple y, por lo tanto, mucho más fácil de probar que es correcto.

Algunas aplicaciones web son susceptibles a una variedad de vulnerabilidades que son introducidas por un diseño y una codificación deficientes, como la inyección de bases de datos y los ataques de secuencias de comandos entre sitios. En estos ataques, las solicitudes pueden manipularse para abusar de la funcionalidad del servidor web.

Puede encontrar más información sobre la evaluación de la seguridad de las TIC en la serie ISO/IEC 15408.

8.29 Pruebas de seguridad en desarrollo y aceptación

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# identificar	#Aplicación_seguridad # Information_securi-ty_assurance # sistema_y_red-trabajo_seguridad	# Proteccion

Control

Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

Propósito

Para validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.

Guia

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deben probarse y verificarse minuciosamente durante los procesos de desarrollo. Las pruebas de seguridad deben ser una parte integral de las pruebas de sistemas o componentes.

Las pruebas de seguridad deben realizarse frente a un conjunto de requisitos, que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad deben incluir pruebas de:

a) funciones de seguridad [por ejemplo, autenticación de usuario (ver8.5), restricción de acceso (ver8.3) y el uso de la criptografía (ver8.24)];

b) codificación segura (ver8.28);

c) configuraciones seguras (ver8.9 ,8.20 y8.22) incluido el de los sistemas operativos, cortafuegos y otros componentes de seguridad.

Los planes de prueba deben determinarse utilizando un conjunto de criterios. El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo. El plan de prueba debe incluir:

a) cronograma detallado de actividades y pruebas;

b) insumos y productos esperados bajo una variedad de condiciones;

c) criterios para evaluar los resultados;

d) decisión de acciones adicionales según sea necesario.

La organización puede aprovechar las herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidades, y debe verificar la corrección de los defectos relacionados con la seguridad.

Para los desarrollos internos, estas pruebas deben ser realizadas inicialmente por el equipo de desarrollo. Luego, se deben realizar pruebas de aceptación independientes para garantizar que el sistema funcione como se espera y solo como se espera (ver5.8). Se debe considerar lo siguiente:

a) realizar actividades de revisión de código como un elemento relevante para probar fallas de seguridad, incluidas entradas y condiciones no anticipadas;

b) realizar un escaneo de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) realizar pruebas de penetración para identificar código y diseño inseguros.

Para los componentes de compra y desarrollo subcontratados, se debe seguir un proceso de adquisición. Los contratos con el proveedor deben abordar los requisitos de seguridad identificados (ver5.20). Los productos y servicios deben evaluarse según estos criterios antes de la adquisición.

Las pruebas deben realizarse en un entorno de prueba que coincida lo más posible con el entorno de producción de destino para garantizar que el sistema no presente vulnerabilidades en el entorno de la organización y que las pruebas sean confiables (ver8.31).

Otra información

Se pueden establecer varios entornos de prueba, que se pueden utilizar para diferentes tipos de pruebas (por ejemplo, pruebas funcionales y de rendimiento). Estos diferentes entornos pueden ser virtuales, con configuraciones individuales para simular una variedad de entornos operativos.

También se deben considerar las pruebas y el monitoreo de los entornos de prueba, las herramientas y las tecnologías para garantizar la eficacia de las pruebas. Las mismas consideraciones se aplican al monitoreo de los sistemas de monitoreo implementados en entornos de desarrollo, prueba y producción. Se necesita juicio, guiado por la sensibilidad de los sistemas y los datos, para determinar cuántas capas de meta-test son útiles.

8.30 Desarrollo subcontratado

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo # Detective	# Confidencialidad # Integridad # Disponibilidad	# Identificar # Proteger # Detectar	# Sistema_y_red_ seguridad #Aplicación_seguridad #Proveedores_relaciones_seguridad	# Gobernanza_y_ Ecosistema # Proteccion

Control

La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

Propósito

Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados.

Guia

Cuando se subcontrata el desarrollo del sistema, la organización debe comunicar y acordar los requisitos y expectativas, y monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Se deben considerar los siguientes puntos en toda la cadena de suministro externa de la organización:

a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado (ver 5.32);

b) requisitos contractuales para prácticas seguras de diseño, codificación y prueba (ver 8.25 para 8.29);

c) provisión del modelo de amenaza para ser considerado por desarrolladores externos;

d) pruebas de aceptación de la calidad y precisión de los entregables (ver 8.29);

e) suministro de pruebas de que se han establecido los niveles mínimos aceptables de seguridad y capacidades de privacidad (p. ej., informes de garantía);

f) provisión de evidencia de que se han aplicado suficientes pruebas para protegerse contra la presencia de contenido malicioso (tanto intencional como no intencional) en el momento de la entrega;

g) provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas;

h) acuerdos de depósito en garantía para el código fuente del software (por ejemplo, si el proveedor cierra);

i) derecho contractual a auditar procesos y controles de desarrollo;

j) requisitos de seguridad para el entorno de desarrollo (ver 8.31);

k) teniendo en cuenta la legislación aplicable (por ejemplo, sobre protección de datos personales).

Otra información

Puede encontrar más información sobre las relaciones con los proveedores en la serie ISO/IEC 27036.

8.31 Separación de los entornos de desarrollo, prueba y producción

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red- trabajo_seguridad	# Proteccion

Control

Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.

Propósito

Para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.

Guia

Debe identificarse e implementarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción.

Se deben considerar los siguientes elementos:

a) separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios (por ejemplo, en entornos físicos o virtuales separados);

b) definir, documentar e implementar reglas y autorizaciones para el despliegue de software desde el estado de desarrollo hasta el de producción;

c) probar los cambios en los sistemas de producción y las aplicaciones en un entorno de prueba o ensayo antes de aplicarlos a los sistemas de producción (ver8.29);

d) no realizar pruebas en entornos de producción excepto en circunstancias que hayan sido definidas y aprobadas;

e) compiladores, editores y otras herramientas de desarrollo o programas de utilidad que no sean accesibles desde los sistemas de producción cuando no se requieran;

f) mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error;

g) no copiar información confidencial en los entornos del sistema de desarrollo y prueba a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y prueba.

En todos los casos, los entornos de desarrollo y pruebas deben protegerse teniendo en cuenta:

a) aplicación de parches y actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas);

b) configuración segura de sistemas y software;

c) control de acceso a los ambientes;

d) seguimiento de cambios en el entorno y código almacenado en el mismo;

e) monitoreo seguro de los ambientes;

f) realizar copias de seguridad de los entornos.

Una sola persona no debe tener la capacidad de realizar cambios tanto en el desarrollo como en la producción sin una revisión y aprobación previas. Esto se puede lograr, por ejemplo, mediante la segregación de los derechos de acceso o mediante reglas supervisadas. En situaciones excepcionales, se deben implementar medidas adicionales como registro detallado y monitoreo en tiempo real para detectar y actuar sobre cambios no autorizados.

Otra información

Sin medidas y procedimientos adecuados, los desarrolladores y evaluadores que tienen acceso a los sistemas de producción pueden presentar riesgos significativos (por ejemplo, modificación no deseada de los archivos o del entorno del sistema, falla del sistema, ejecución de código no autorizado y no probado en los sistemas de producción, divulgación de datos confidenciales, integridad de datos y problemas de disponibilidad). Es necesario mantener un entorno conocido y estable en el que realizar pruebas significativas y evitar el acceso inapropiado del desarrollador al entorno de producción.

Las medidas y los procedimientos incluyen roles cuidadosamente diseñados junto con la implementación de requisitos de segregación de tareas y la implementación de procesos de monitoreo adecuados.

El personal de desarrollo y pruebas también representa una amenaza para la confidencialidad de la información de producción. Las actividades de desarrollo y prueba pueden provocar cambios no deseados en el software o la información si comparten el mismo entorno informático. Por lo tanto, es deseable separar los entornos de desarrollo, prueba y producción para reducir el riesgo de cambios accidentales o acceso no autorizado al software de producción y los datos comerciales (ver8.33 para la protección de la información de prueba).

En algunos casos, la distinción entre entornos de desarrollo, prueba y producción se puede desdibujar deliberadamente y las pruebas se pueden llevar a cabo en un entorno de desarrollo o mediante implementaciones controladas para usuarios o servidores reales (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, la prueba del producto puede ocurrir mediante el uso en vivo del producto dentro de la organización. Además, para reducir el tiempo de inactividad de las implementaciones en vivo, se pueden admitir dos entornos de producción idénticos donde solo uno está en vivo en cualquier momento.

Procesos de soporte para el uso de datos de producción en entornos de desarrollo y prueba (8.33) son necesarios.

Las organizaciones también pueden considerar la orientación proporcionada en esta sección para los entornos de capacitación al realizar la capacitación del usuario final.

8.32 Gestión de cambios

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#Aplicación_seguridad # sistema_y_red- trabajo_seguridad	# Proteccion

Control

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

Propósito

Preservar la seguridad de la información al ejecutar cambios.

Guia

La introducción de nuevos sistemas y cambios importantes en los sistemas existentes debe seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación administrada. Deben existir responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de procesamiento de información y los sistemas de información, durante todo el ciclo de vida del desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

Siempre que sea factible, deben integrarse los procedimientos de control de cambios para la infraestructura y el software de las TIC.

Los procedimientos de control de cambios deben incluir:

a) planificar y evaluar el impacto potencial de los cambios considerando todas las dependencias;

b) autorización de cambios;

c) comunicar los cambios a las partes interesadas pertinentes;

d) pruebas y aceptación de pruebas para los cambios (ver8.29);

e) implementación de cambios, incluidos los planes de implementación;

f) consideraciones de emergencia y contingencia, incluidos los procedimientos de respaldo;

g) mantener registros de cambios que incluyan todo lo anterior;

h) asegurar que la documentación operativa (ver5.37) y los procedimientos de usuario se modifican según sea necesario para seguir siendo apropiados;

i) garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (ver5.30) se modifican según sea necesario para seguir siendo apropiados.

Otra información

El control inadecuado de los cambios en las instalaciones de procesamiento de información y los sistemas de información es una causa común de fallas en el sistema o en la seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere software del entorno de desarrollo al operativo, pueden afectar la integridad y disponibilidad de las aplicaciones.

Cambiar el software puede afectar el entorno de producción y viceversa.

Las buenas prácticas incluyen la prueba de los componentes de las TIC en un entorno segregado de los entornos de producción y desarrollo (ver8.31). Esto proporciona un medio para tener control sobre el nuevo software y permitir una protección adicional de la información operativa que se utiliza con fines de prueba. Esto debería incluir parches, paquetes de servicio y otras actualizaciones.

El entorno de producción incluye sistemas operativos, bases de datos y plataformas de middleware. El control debe aplicarse para cambios de aplicaciones e infraestructuras.

8.33 Información de prueba

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad	# Proteger	# Información_protección	# Proteccion

Control

La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.

Propósito

Para garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

Guia

La información de prueba debe seleccionarse para garantizar la confiabilidad de los resultados de la prueba y la confidencialidad de la información operativa relevante. La información confidencial (incluida la información de identificación personal) no debe copiarse en los entornos de desarrollo y prueba (consulte8.31).

Se deben aplicar las siguientes pautas para proteger las copias de la información operativa, cuando se utilizan con fines de prueba, ya sea que el entorno de prueba se construya internamente o en un servicio en la nube:

a) aplicar los mismos procedimientos de control de acceso a los entornos de prueba que los que se aplican a los entornos operativos;

b) tener una autorización separada cada vez que se copia información operativa a un entorno de prueba;

c) registrar la copia y el uso de información operativa para proporcionar una pista de auditoría;

d) proteger la información confidencial mediante su eliminación o enmascaramiento (ver8.11) si se utiliza para pruebas;

e) eliminar correctamente (ver8.10) información operativa de un entorno de prueba inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de la prueba.

La información de la prueba debe almacenarse de forma segura (para evitar la manipulación, que de lo contrario puede generar resultados no válidos) y solo debe usarse para fines de prueba.

Otra información

Las pruebas del sistema y de aceptación pueden requerir volúmenes sustanciales de información de prueba que estén lo más cerca posible de la información operativa.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Sistema_y_red_ seguridad # Información_protección	# Gobernanza_y_ Ecosistema # Protección ción

Control

Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

Propósito

Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos comerciales.

Guia

Se deben observar las siguientes pautas:

a) acordar solicitudes de auditoría para el acceso a sistemas y datos con la gestión adecuada;

b) acordar y controlar el alcance de las pruebas de auditoría técnica;

c) limitar las pruebas de auditoría al acceso de solo lectura al software y los datos. Si el acceso de solo lectura no está disponible para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor;

d) si se otorga el acceso, establecer y verificar los requisitos de seguridad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo, computadoras portátiles o tabletas) antes de permitir el acceso;

e) solo permitir el acceso que no sea de solo lectura para copias aisladas de archivos del sistema, eliminándolos cuando se complete la auditoría, o brindándoles la protección adecuada si existe la obligación de mantener dichos archivos bajo los requisitos de documentación de auditoría;

f) identificar y acordar solicitudes de procesamiento especial o adicional, como ejecutar herramientas de auditoría;

g) ejecutar pruebas de auditoría que puedan afectar la disponibilidad del sistema fuera del horario comercial;

h) supervisar y registrar todos los accesos con fines de auditoría y prueba.

Otra información

Las pruebas de auditoría y otras actividades de aseguramiento también pueden ocurrir en los sistemas de prueba y desarrollo, donde tales pruebas pueden afectar, por ejemplo, la integridad del código o conducir a la divulgación de cualquier información confidencial que se encuentre en dichos entornos.

Anexo A
(informativo)

Usando atributos

A.1 Generalidades

Este anexo proporciona una tabla para demostrar el uso de atributos como una forma de crear diferentes vistas de los controles. Los cinco ejemplos de atributos son (ver4.2):

a) Tipos de control (#Preventivo, #Detectivo, #Correctivo)

b) Propiedades de seguridad de la información (#Confidencialidad, #Integridad, #Disponibilidad)

c) Conceptos de ciberseguridad (#Identificar, #Proteger, #Detectar, #Responder, #Recuperar)

d) Capacidades operativas (#Gobernanza, #Gestión_de_activos, #Protección_de_la_información, #Seguridad_de_recursos_humanos, #Seguridad_física, #Seguridad_de_sistemas_y_redes, #Seguridad_de_aplicaciones, # Configuración_segura, # Gestión_de_identidad_y_acceso, # Gestión_de_amenazas_y_vulnerabilidades, #Continuidad, #Seguridad_de_relaciones_con_proveedores, #Cumplimiento_y_legal, # Gestión_de_eventos_de_seguridad_de_la_información, #Garantía_de_seguridad_de_la_información)

e) Dominios de seguridad (#Gobernanza_y_Ecosistema, #Protección, #Defensa, #Resiliencia)

Tabla A.1 contiene una matriz de todos los controles en este documento con sus valores de atributo dados.

El filtrado o clasificación de la matriz se puede lograr mediante el uso de una herramienta como una hoja de cálculo simple o una base de datos, que puede incluir más información como texto de control, orientación, orientación o atributos específicos de la organización (verA.2).

Tabla A.1 - Matriz de controles y valores de atributos

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.1	Políticas para información seguridad	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_ y_Ecosys- artículo # Resil- iencia
5.2	Información roles de seguridad y responsabilidad Habilidades	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernar- ance_y_ Ecosistema # Proteccion # Resiliencia
5.3	segregación de deberes	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Gobernanza # Identidad_y_ access_man- gestion	# Gobernanza_ y_Ecosys- tiempo
5.4	Gestión responsable corbatas	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_ y_Ecosys- tiempo
5.5	Contactar con autoridades	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar #Responder # recuperar	# Gobernanza	# Defensa # Re- silencio

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.6	Contactar con inter especial son grupos	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Responder # Recubrir	# Gobernanza	# Defensa
5.7	Inteligencia de amenazas gencia	# Preventivo # Detective # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Detectar #Responder	# amenaza_y_ vulnerabilidad_ administración	# Defensa # Resilencio
5.8	Información seguridad en hombre del proyecto - gestion	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Protectar	# Gobernanza	# Gobernanza_ y_Ecosys- artículo # ción
5.9	Inventario de información y otra asociado activos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Asset_man- gestion	# Gobernanza_ y_Ecosys- artículo # ción
5.10	Uso aceptable de información y otra asociado activos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_man- gestion # Información_ proteccion	# Gobernanza_ y_Ecosys- artículo # ción
5.11	Retorno de activos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_man- gestion	# Proteccion
5.12	Clasificación de información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Información_ proteccion	# Proteccion # Defensa
5.13	Etiquetado de información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Información_ proteccion	# Defensa # Proteccion
5.14	Información transferir	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_man- gestion # Información_ proteccion	# Proteccion
5.15	Control de acceso	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.16	hombre de identidad- gestion	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.17	Autenticación información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.18	Derechos de acceso	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.19	Información seguridad en relación con el proveedor naciones	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.20	Direccionamiento información seguridad con- en proveedor acuerdos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción
5.21	Gerente información seguridad en la oferta TIC cadena	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción
5.22	Monitor- ing, revisión y cambio administración de proveedor servicios	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción #Defensa # Información_ seguridad_como- seguro
5.23	Información seguridad para uso de la nube servicios	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción
5.24	Información incidente de seguridad manejo de abolladuras - planeación mental y prepara- ción	# Correctivo	# Confidencial- #Integridad # Disponibilidad	# Responder # Re- cubrir	# Gobernanza # Informa- tion_securi- ty_event_man- gestion	# Defensa
5.25	Evaluación y decisión sobre información ción de seguridad eventos	# Detective	# Confidencial- #Integridad # Disponibilidad	# Detectar # Re- responder	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.26	Respuesta a información incidente de seguridad abolladuras	# Correctivo	# Confidencial- #Integridad # Disponibilidad	# Responder # Re- cubrir	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.27	Aprendiendo de información incidente de seguridad abolladuras	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.28	Colección de evidencia	# Correctivo	# Confidencial- #Integridad # Disponibilidad	# Detectar # Re- responder	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.29	Información seguridad durante- en interrupción	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Re- responder	# Continuidad	# Proteccion # Resiliencia
5.30	preparación para las TIC para negocios continuidad	# Correctivo	# Disponibilidad	# Responder	# Continuidad	# Resiliencia

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.31	legal, estatutario ry, regulador y contrato- requerimiento tual mentos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	#Legal_y_ cumplimiento	# Gobernanza_ y_Ecosys- artículo # ción
5.32	Intelectual propiedad derechos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	#Legal_y_ cumplimiento	# Gobernanza_ y_Ecosys- tiempo
5.33	Proteccion DE registros	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	#Legal_y_ cumplimiento # Asset_man- gestion # Información_ proteccion	# Defensa
5.34	Privacidad y proteccion DE información personal	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Información_ proteccion #Legal_y_ cumplimiento	# Proteccion
5.35	Independiente repaso de información seguridad	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Información_ seguridad_como- seguro	# Gobernanza_ y_Ecosys- tiempo
5.36	Cumplimiento con políticas, reglas y normas para información seguridad	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	#Legal_y_ cumplimiento # Información_ seguridad_como- seguro	# Gobernanza_ y_Ecosys- tiempo
5.37	documentado operando procedimientos	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Re- cubrir	# Asset_man- gestion # fisio- cal_seguridad # Sistema_y_ network_secu- ridad # Aplica- ción_seguridad # Secure_con- figuración # Identidad_ y_acceso_ administración # amenaza_y_ vulnerabilidad_ administración # Continuidad # Informa- tion_securi- ty_event_man- gestion	# Gobernanza_ y_Ecosys- artículo # ción #Defensa
6.1	Poner en pantalla	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Human_re- source_secu- ridad	# Gobernanza_ y_Ecosys- tiempo

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
6.2	Términos y condiciones de empleo	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Human_resource_seguridad	# Gobernanza_y_Ecosys-tiempo
6.3	Información seguridad conciencia, educación y capacitación	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Human_resource_seguridad	# Gobernanza_y_Ecosys-tiempo
6.4	Disciplinario proceso	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Responder	# Human_resource_seguridad	# Gobernanza_y_Ecosys-tiempo
6.5	responsabilidad Habilidades después terminación o cambio de empleo	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Human_resource_seguridad #Activo_administración	# Gobernanza_y_Ecosys-tiempo
6.6	confiadolidad o no divulgación acuerdos	# Preventivo	# Confidencial alidad	# Proteger	# Human_resource_security #Information_protección # Proveedor_relaciones	# Gobernanza_y_Ecosys-tiempo
6.7	Trabajo remoto- En g	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_mangestion # Información_proteccion # Physical_seseguridad # System_and_net-trabajo_seguridad	# Proteccion
6.8	Información evento de seguridad reportando	# Detective	# Confidencial- #Integridad # Disponibilidad	# Detectar	# Information_security_event_mangestion	# Defensa
7.1	Seguridad física perimetral- tercera	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_seseguridad	# Proteccion
7.2	Entrada física	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_seseguridad # Identity_and_Access_Management	# Proteccion
7.3	Oficina de seguridad es, habitaciones y instalaciones	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_secalidad #Activo_administración	# Proteccion
7.4	Seguridad física monitor de rity- En g	# Preventivo # Detective	# Confidencial- #Integridad # Disponibilidad	# Proteger # Detectar	# Physical_seseguridad	# Proteccion # Defensa

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
7.5	Proteger-en contra físico y ambiental amenazas	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-seguridad	# Proteccion
7.6	Trabajando en áreas seguras	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-seguridad	# Proteccion
7.7	Limpiar el escritorio y pantalla clara	# Preventivo	# Confidencial alidad	# Proteger	# Physical_se-seguridad	# Proteccion
7.8	Equipo ubicación y proteccion	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion
7.9	seguridad de as-pone en marcha ises	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion
7.10	Medios de almacenamiento	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion
7.11	Secundario utilidades	# Preventivo # Detective	# Integridad # Disponibilidad	# Proteger # De-tectar	# Physical_se-seguridad	# Proteccion
7.12	Cableado seguro ridad	# Preventivo	# Confidencial alidad # disponible-habilidad	# Proteger	# Physical_se-seguridad	# Proteccion
7.13	Equipo mantenimiento	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion # Resiliencia
7.14	Eliminación segura al o reutilización de equipo	# Preventivo	# Confidencial alidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion
8.1	Punto final de usuario dispositivos	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Asset_man-gestion # Información_ proteccion	# Proteccion
8.2	Privilegiado derechos de acceso	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion
8.3	Información Restricción de acceso-ción	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion
8.4	El acceso a los código fuente	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Identidad_ y_acceso_ administración # Aplica-ción_seguridad # Secure_con-figuración	# Proteccion
8.5	autenticación segura ticación	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion

Cuadro A.1*(continuado)*

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.6	capacidad hombre-gestion	# Preventivo # Detective	# Integridad # Disponibilidad	# Identificar # Pro-detectar #Detectar	# Continuidad	# Gobernanza_y_Ecosys-artículo # ción
8.7	Proteccion contra mal-Cierto	# Preventivo # Detective # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Proteger # De-tectar	# Sistema_y_network_secu-ridad # Informa-tion_protec-ción	# Proteccion # Defensa
8.8	Gestión de técnico vulnerabilidades	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Identificar # Pro-tectar	# amenaza_y_vulnerabilidad_administración	# Gobernanza_y_Ecosys-artículo # ción #Defensa
8.9	Configuración administración	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Secure_con-figuración	# Proteccion
8.10	Información supresión	# Preventivo	# Confidencial alidad	# Proteger	# Información_proteccion #Legal_y_cumplimiento	# Proteccion
8.11	Enmascaramiento de datos	# Preventivo	# Confidencial alidad	# Proteger	# Información_proteccion	# Proteccion
8.12	Fuga de datos prevención	# Preventivo # Detective	# Confidencial alidad	# Proteger # De-tectar	# Información_proteccion	# Proteccion # Defensa
8.13	Información respaldo	# Correctivo	# Integridad # Disponibilidad	# recuperar	# Continuidad	# Proteccion
8.14	Redundancia de información Procesando instalaciones	# Preventivo	# Disponibilidad	# Proteger	# Continuidad # Asset_man-gestion	# Proteccion # Resiliencia
8.15	Inicio sesión	# Detective	# Confidencial-#Integridad # Disponibilidad	# Detectar	# Informa-tion_securi-ty_event_man-gestion	# Proteccion # Defensa
8.16	Supervisión ocupaciones	# Detective # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Detectar # Re-responder	# Informa-tion_securi-ty_event_man-gestion	# Defensa
8.17	Reloj síncrono nización	# Detective	# Integridad	# Proteger # De-tectar	# Informa-tion_securi-ty_event_man-gestion	# Proteccion # Defensa
8.18	uso de utilidad legítima programas	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Sistema_y_network_secu-rity #Secure_configuración # Solicitud_seguridad	# Proteccion
8.19	Instalación de software en Operacional sistemas	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Secure_con-figuración # Solicitud_seguridad	# Proteccion

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
8.20	Redes seguridad	# Preventivo # Detective	# Confidencial- #Integridad # Disponibilidad	# Proteger # De- tectar	# Sistema_y_ network_secu- ridad	# Proteccion
8.21	Seguridad de servicio de red vicios	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.22	segregación de redes	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.23	Filtrado web	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.24	Uso de crip- tografia	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Secure_con- figuración	# Proteccion
8.25	desarrollo seguro opment vida ciclo	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion
8.26	Solicitud re-seguridad requisitos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion # Defensa
8.27	sistema seguro arquitectura e ingeniero- principios de formación	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion
8.28	Codificación segura	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion
8.29	Seguridad prueba en de- desarrollo y aceptación	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Aplica- ción_seguridad # Informa- tion_securi- ty_assurance # Sistema_y_ network_secu- ridad	# Proteccion
8.30	subcontratado desarrollo	# Preventivo # Detective	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- detectar #Detectar	# Sistema_y_ network_secu- ridad # Aplica- ción_seguridad # Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción

Cuadro A.1*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
8.31	Separación de desarrollo-prueba, prueba y producción ambientes	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Aplica-ción_seguridad # Sistema_y_network_secu-ridad	# Proteccion
8.32	Cambia hombre - gestion	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Aplica-ción_seguridad # Sistema_y_network_secu-ridad	# Proteccion
8.33	Prueba de información ción	# Preventivo	# Confidencial-#Integridad	# Proteger	# Información_proteccion	# Proteccion
8.34	Proteccion de información sistemas de ción durante la auditoría pruebas	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Sistema_y_network_secu-ridad # Informa-tion_protec-ción	# Gobernanza_y_Ecosys-artículo # ción

Tabla A.2 muestra un ejemplo de cómo crear una vista filtrando por un valor de atributo particular, en este caso #Corrective.

Tabla A.2 - Vista de #Controles Correctivos

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.5	Contactar con autoridades	# Preventivo # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Identificar # Pro-tectar #Responder # recuperar	# Gobernanza	# Defensa # Re-silencio
5.6	Contactar con inter especial son grupos	# Preventivo # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Proteger # Responder # Re-cubrir	# Gobernanza	# Defensa
5.7	Inteligencia de amenazas gencia	# Preventivo # Detective # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Identificar # Des-tectar #Responder	# amenaza_y_vulnerabilidad_administración	# Defensa # Re-silencio
5.24	Información incidente de seguridad manejo de abolladuras - planeación mental y prepara-ción	# Correctivo	# Confidencial-#Integridad # Disponibilidad	# Responder # Re-cubrir	# Gobernanza # Informa-tion_securi-ty_event_man-gestion	# Defensa
5.26	Respuesta a información incidente de seguridad abolladuras	# Correctivo	# Confidencial-#Integridad # Disponibilidad	# Responder # Re-cubrir	# Informa-tion_securi-ty_event_man-gestion	# Defensa
5.28	Colección de evidencia	# Correctivo	# Confidencial-#Integridad # Disponibilidad	# Detectar # Re-responder	# Informa-tion_securi-ty_event_man-gestion	# Defensa
5.29	Información seguridad durante-en interrupción	# Preventivo # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Proteger # Re-responder	# Continuidad	# Proteccion # Resiliencia

Cuadro A.2*(continuado)*

YO ASI / **CEI 27002 control identificar**	**nombre de control**	**Tipo de control**	**Información seguridad propiedades**	**La seguridad cibernética conceptos**	**Operacional capacidades**	**Seguridad dominios**
5.30	preparación para las TIC para negocios continuidad	# Correctivo	# Disponibilidad	# Responder	# Continuidad	# Resiliencia
5.35	Independiente repaso de información seguridad	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Protectar	# Información_ seguridad_como- seguro	# Gobernanza_ y_Ecosys- tiempo
5.37	documentado operando procedimientos	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Recubrir	# Asset_man- gestion # fisio- cal_seguridad # Sistema_y_ network_secu- ridad # Aplica- ción_seguridad # Secure_con- figuración # Identidad_ y_acceso_ administración # amenaza_y_ vulnerabilidad_ administración # Continuidad # Informa- tion_securi- ty_event_man- gestion	# Gobernanza_ y_Ecosys- artículo # ción #Defensa
6.4	Disciplinario proceso	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Responder	# Human_re- source_secu- ridad	# Gobernanza_ y_Ecosys- tiempo
8.7	Proteccion contra mal- Cierto	# Preventivo # Detective # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Detectar	# Sistema_y_ network_secu- ridad # Informa- tion_protec- ción	# Proteccion # Defensa
8.13	Información respaldo	# Correctivo	# Integridad # Disponibilidad	# recuperar	# Continuidad	# Proteccion
8.16	Supervisión ocupaciones	# Detective # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Detectar # Responder	# Informa- tion_securi- ty_event_man- gestion	# Defensa

A.2 Puntos de vista organizacionales

Dado que los atributos se utilizan para crear diferentes vistas de controles, las organizaciones pueden descartar los ejemplos de atributos propuestos en este documento y crear sus propios atributos con diferentes valores para abordar necesidades específicas en la organización. Además, los valores asignados a cada atributo pueden diferir entre organizaciones ya que las organizaciones pueden tener diferentes puntos de vista sobre el uso o la aplicabilidad del control o de los valores asociados al atributo (cuando los valores son específicos del contexto). de la organización). El primer paso es comprender por qué es deseable un atributo específico de la organización. Por ejemplo, si una organización ha construido sus planes de tratamiento de riesgos [consulte ISO / IEC 27001: 2013, 6.1.3 e)] en función de los eventos, es posible que desee asociar un atributo de escenario de riesgo a cada control en este documento.

El beneficio de tal atributo es acelerar el proceso de cumplimiento del requisito ISO/IEC 27001 relacionado con el tratamiento de riesgos, que consiste en comparar los controles determinados a través del proceso de tratamiento de riesgos (denominados controles "necesarios"), con aquellos en ISO / IEC 27001: 2013, Anexo A (que se emiten en este documento) para garantizar que no se ha pasado por alto ningún control necesario.

Una vez que se conocen el propósito y los beneficios, el siguiente paso es determinar los valores de los atributos. Por ejemplo, la organización podría identificar 9 eventos:

1) pérdida o robo del dispositivo móvil;

2) pérdida o robo de las instalaciones de la organización;

3) fuerza mayor, vandalismo y terrorismo;

4) falla de software, hardware, energía, internet y comunicaciones;

5) fraude;

6) piratería;

7) divulgación;

8) incumplimiento de la ley;

9) ingeniería social.

Por lo tanto, el segundo paso se puede lograr asignando identificadores a cada evento (por ejemplo, E1, E2, ..., E9).

El tercer paso es copiar los identificadores de control y los nombres de control de este documento en una hoja de cálculo o base de datos y asociar los valores de atributo con cada control, recordando que cada control puede tener más de un valor de atributo.

El paso final es ordenar la hoja de cálculo o consultar la base de datos para extraer la información requerida.

Otros ejemplos de atributos organizacionales (y valores posibles) incluyen:

a) madurez (valores de la serie ISO/IEC 33000 u otros modelos de madurez);

b) estado de implementación (pendiente, en proceso, parcialmente implementado, completamente implementado);

c) prioridad (1, 2, 3, etc.);

d) áreas organizacionales involucradas (seguridad, TIC, recursos humanos, alta dirección, etc.);

e) eventos;

f) bienes involucrados;

e) construir y ejecutar, para diferenciar los controles utilizados en los diferentes pasos del ciclo de vida del servicio;

g) otros marcos con los que trabaja la organización o desde los que puede estar en transición.

Anexo B
(informativo)

Correspondencia de ISO/IEC 27002:2022 (este documento) con ISO/IEC 27002: 2013

El propósito de este anexo es proporcionar compatibilidad con versiones anteriores de ISO/IEC 27002: 2013 para las organizaciones que actualmente usan ese estándar y ahora desean hacer la transición a esta edición.

Tabla B.1 proporciona la correspondencia de los controles especificados enCláusulas 5 para8 con los de la norma ISO/IEC 27002:2013.

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / **CEI 27002: 2022 control identificar**	**ISO / CEI 27002: 2013 identificador de control**	**nombre de control**
5.1	05.1.1, 05.1.2	Políticas de seguridad de la información
5.2	06.1.1	Roles y responsabilidades de seguridad de la información
5.3	06.1.2	Segregación de deberes
5.4	07.2.1	responsabilidades de gestión
5.5	06.1.3	Contacto con autoridades
5.6	06.1.4	Contacto con grupos de interés especial
5.7	Nuevo	Inteligencia de amenazas
5.8	06.1.5, 14.1.1	Seguridad de la información en la gestión de proyectos.
5.9	08.1.1, 08.1.2	Inventario de información y otros activos asociados
5.10	08.1.3, 08.2.3	Uso aceptable de la información y otros activos asociados
5.11	08.1.4	Devolución de activos
5.12	08.2.1	Clasificación de la información
5.13	08.2.2	Etiquetado de información
5.14	13.2.1, 13.2.2, 13.2.3	Transferencia de información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de identidad
5.17	09.2.4, 09.3.1, 09.4.3	Información de autenticación
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso
5.19	15.1.1	Seguridad de la información en las relaciones con los proveedores
5.20	15.1.2	Abordar la seguridad de la información en los acuerdos con los proveedores
5.21	15.1.3	Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22	15.2.1, 15.2.2	Seguimiento, revisión y gestión de cambios de servicios de proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25	16.1.4	Evaluación y decisión sobre eventos de seguridad de la información

Tabla B.1*(continuado)*

YO ASI / **CEI 27002: 2022 control identificar**	**ISO / CEI 27002: 2013 identificador de control**	**nombre de control**
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de los incidentes de seguridad de la información
5.28	16.1.7	Recolección de evidencia
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de las TIC para la continuidad del negocio
5.31	18.1.1, 18.1.5	Requisitos legales, estatutarios, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual
5.33	18.1.3	Protección de registros
5.34	18.1.4	Privacidad y protección de PII
5.35	18.2.1	Revisión independiente de la seguridad de la información.
5.36	18.2.2, 18.2.3	Cumplimiento de políticas, normas y estándares de seguridad de la información
5.37	12.1.1	Procedimientos operativos documentados
6.1	07.1.1	Poner en pantalla
6.2	07.1.2	Términos y condiciones de empleo
6.3	07.2.2	Concientización, educación y capacitación en seguridad de la información
6.4	07.2.3	Proceso Disciplinario
6.5	07.3.1	Responsabilidades después de la terminación o cambio de empleo
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Trabajo remoto
6.8	16.1.2, 16.1.3	Informes de eventos de seguridad de la información
7.1	11.1.1	Perímetros físicos de seguridad
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Asegurar oficinas, salas e instalaciones
7.4	Nuevo	Monitoreo de seguridad física
7.5	11.1.4	Protección contra amenazas físicas y ambientales.
7.6	11.1.5	Trabajar en áreas seguras
7.7	11.2.9	Escritorio despejado y pantalla despejada
7.8	11.2.1	Emplazamiento y protección de equipos
7.9	11.2.6	Seguridad de los activos fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Medios de almacenamiento
7.11	11.2.2	Utilidades de apoyo
7.12	11.2.3	seguridad del cableado
7.13	11.2.4	Mantenimiento de equipo
7.14	11.2.7	Eliminación segura o reutilización de equipos
8.1	06.2.1, 11.2.8	Dispositivos de punto final de usuario
8.2	09.2.3	Derechos de acceso privilegiado
8.3	09.4.1	Restricción de acceso a la información
8.4	09.4.5	Acceso al código fuente
8.5	09.4.2	Autenticación segura
8.6	12.1.3	Gestión de capacidad
8.7	12.2.1	Protección contra malware

Tabla B.1*(continuado)*

YO ASI / **CEI 27002: 2022 control identificar**	**ISO / CEI 27002: 2013 identificador de control**	**nombre de control**
8.8	12.6.1, 18.2.3	Gestión de vulnerabilidades técnicas
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Eliminación de información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de fuga de datos
8.13	12.3.1	Copia de seguridad de la información
8.14	17.2.1	Redundancia de las instalaciones de procesamiento de información
8.15	12.4.1, 12.4.2, 12.4.3	Inicio sesión
8.16	Nuevo	Actividades de seguimiento
8.17	12.4.4	Sincronización de reloj
8.18	09.4.4	Uso de programas de utilidad privilegiados
8.19	12.5.1, 12.6.2	Instalación de software en sistemas operativos
8.20	13.1.1	Seguridad en redes
8.21	13.1.2	Seguridad de los servicios de red.
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado web
8.24	10.1.1, 10.1.2	Uso de criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de la aplicación
8.27	14.2.5	Principios de arquitectura e ingeniería de sistemas seguros
8.28	Nuevo	Codificación segura
8.29	14.2.8, 14.2.9	Pruebas de seguridad en desarrollo y aceptación.
8.30	14.2.7	Desarrollo subcontratado
8.31	12.1.4, 14.2.6	Separación de los entornos de desarrollo, prueba y producción
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestión del cambio
8.33	14.3.1	Información de prueba
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

Tabla B.2 proporciona la correspondencia de los controles especificados en ISO/IEC 27002:2013 con los de este documento.

Tabla B.2 - Correspondencia entre controles en ISO/IEC 27002:2013 y controles en esta documento

ISO / CEI 27002: 2013 control identificar	YO ASI / **CEI 27002: 2022 identificador de control**	**Nombre de control según ISO/IEC 27002:2013**
5		Políticas de seguridad de la información
5.1		Dirección de gestión para la seguridad de la información.
5.1.1	5.1	Políticas de seguridad de la información
5.1.2	5.1	Revisión de las políticas de seguridad de la información
6		Organización de la seguridad de la información.

Tabla B.2*(continuado)*

ISO / CEI 27002: 2013 control identificar	YO ASI / CEI 27002: 2022 identificador de control	Nombre de control según ISO/IEC 27002:2013
6.1		Organización interna
6.1.1	5.2	Roles y responsabilidades de seguridad de la información
6.1.2	5.3	Segregación de deberes
6.1.3	5.5	Contacto con autoridades
6.1.4	5.6	Contacto con grupos de interés especial
6.1.5	5.8	Seguridad de la información en la gestión de proyectos.
6.2		Dispositivos móviles y teletrabajo
6.2.1	8.1	política de dispositivos móviles
6.2.2	6.7	teletrabajo
7		seguridad de los recursos humanos
7.1		Antes del empleo
7.1.1	6.1	Poner en pantalla
7.1.2	6.2	Términos y condiciones de empleo
7.2		Durante el empleo
7.2.1	5.4	responsabilidades de gestión
7.2.2	6.3	Concientización, educación y capacitación en seguridad de la información
7.2.3	6.4	Proceso Disciplinario
7.3		Terminación y cambio de empleo
7.3.1	6.5	Terminación o cambio de responsabilidades laborales
8		Gestión de activos
8.1		Responsabilidad por los activos
8.1.1	5.9	Inventario de activos
8.1.2	5.9	Propiedad de los activos
8.1.3	5.10	Uso aceptable de los activos
8.1.4	5.11	Devolución de activos
8.2		Clasificación de la información
8.2.1	5.12	Clasificación de la información
8.2.2	5.13	Etiquetado de información
8.2.3	5.10	manejo de activos
8.3		manejo de medios
8.3.1	7.10	Gestión de medios extraíbles
8.3.2	7.10	Eliminación de medios
8.3.3	7.10	Transferencia de medios físicos
9		Control de acceso
9.1		Requisitos comerciales de control de acceso
9.1.1	5.15	Política de control de acceso
9.1.2	5.15	Acceso a redes y servicios de red
9.2		Gestión de acceso de usuarios
9.2.1	5.16	Alta y baja de usuario
9.2.2	5.18	Aprovisionamiento de acceso de usuarios
9.2.3	8.2	Gestión de derechos de acceso privilegiado
9.2.4	5.17	Gestión de la información secreta de autenticación de los usuarios

Tabla B.2*(continuado)*

ISO / CEI 27002: 2013 control identificar	YO ASI / CEI 27002: 2022 identificador de control	Nombre de control según ISO/IEC 27002:2013
9.2.5	5.18	Revisión de los derechos de acceso de los usuarios
9.2.6	5.18	Eliminación o ajuste de los derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de información de autenticación secreta
9.4		Control de acceso a sistemas y aplicaciones
9.4.1	8.3	Restricción de acceso a la información
9.4.2	8.5	Procedimientos seguros de inicio de sesión
9.4.3	5.17	Sistema de gestión de contraseñas
9.4.4	8.18	Uso de programas de utilidad privilegiados
9.4.5	8.4	Control de acceso al código fuente del programa
10		Criptografía
10.1		Controles criptográficos
10.1.1	8.24	Política sobre el uso de controles criptográficos
10.1.2	8.24	Gestión de claves
11		Seguridad física y ambiental
11.1		Áreas seguras
11.1.1	7.1	Perímetro de seguridad física
11.1.2	7.2	Controles de entrada física
11.1.3	7.3	Asegurar oficinas, salas e instalaciones
11.1.4	7.5	Protección contra amenazas externas y ambientales.
11.1.5	7.6	Trabajar en áreas seguras
11.1.6	7.2	Zonas de entrega y carga
11.2		Equipo
11.2.1	7.8	Emplazamiento y protección de equipos
11.2.2	7.11	Utilidades de apoyo
11.2.3	7.12	seguridad del cableado
11.2.4	7.13	Mantenimiento de equipo
11.2.5	7.10	Eliminación de activos
11.2.6	7.9	Seguridad de equipos y activos fuera de las instalaciones
11.2.7	7.14	Eliminación segura o reutilización de equipos
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de escritorio despejado y pantalla despejada
12		seguridad de las operaciones
12.1		Procedimientos operativos y responsabilidades
12.1.1	5.37	Procedimientos operativos documentados
12.1.2	8.32	Gestión del cambio
12.1.3	8.6	Gestión de capacidad
12.1.4	8.31	Separación de entornos de desarrollo, pruebas y operativos
12.2		Protección contra malware
12.2.1	8.7	Controles contra malware
12.3		Respaldo
12.3.1	8.13	Copia de seguridad de la información

Tabla B.2*(continuado)*

ISO / CEI 27002: 2013 control identificar	YO ASI / CEI 27002: 2022 identificador de control	Nombre de control según ISO/IEC 27002:2013
12.4		Registro y monitoreo
12.4.1	8.15	El registro de eventos
12.4.2	8.15	Protección de la información de registro
12.4.3	8.15	Registros de administrador y operador
12.4.4	8.17	Sincronización de reloj
12.5		Control de software operativo
12.5.1	8.19	Instalación de software en sistemas operativos
12.6		Gestión de vulnerabilidades técnicas
12.6.1	8.8	Gestión de vulnerabilidades técnicas
12.6.2	8.19	Restricciones en la instalación de software
12.7		Consideraciones de auditoría de sistemas de información
12.7.1	8.34	Controles de auditoría de sistemas de información
13		Seguridad de las comunicaciones
13.1		Instalaciones de gestión de seguridad de red.
13.1.1	8.20	Controles de red
13.1.2	8.21	Seguridad de los servicios de red.
13.1.3	8.22	Segregación en redes
13.2		Transferencia de información
13.2.1	5.14	Políticas y procedimientos de transferencia de información
13.2.2	5.14	Acuerdos de transferencia de información
13.2.3	5.14	mensajería electrónica
13.2.4	6.6	Acuerdos de confidencialidad o no divulgación
14		Adquisición, desarrollo y mantenimiento del sistema
14.1		Requisitos de seguridad de los sistemas de información
14.1.1	5.8	Análisis y especificación de requisitos de seguridad de la información.
14.1.2	8.26	Protección de servicios de aplicaciones en redes públicas
14.1.3	8.26	Protección de transacciones de servicios de aplicaciones
14.2		Seguridad en los procesos de desarrollo y soporte
14.2.1	8.25	Política de desarrollo seguro
14.2.2	8.32	Procedimientos de control de cambios del sistema
14.2.3	8.32	Revisión técnica de aplicaciones tras cambios de plataforma operativa
14.2.4	8.32	Restricciones a los cambios en los paquetes de software
14.2.5	8.27	Principios de ingeniería de sistemas seguros
14.2.6	8.31	Entorno de desarrollo seguro
14.2.7	8.30	Desarrollo subcontratado
14.2.8	8.29	Pruebas de seguridad del sistema
14.2.9	8.29	Pruebas de aceptación del sistema
14.3		Datos de prueba
14.3.1	8.33	Protección de datos de prueba
15		Relaciones con proveedores
15.1		Seguridad de la información en las relaciones con los proveedores
15.1.1	5.19	Política de seguridad de la información en las relaciones con proveedores

Tabla B.2*(continuado)*

ISO / CEI 27002: 2013 control identificar	YO ASI / CEI 27002: 2022 identificador de control	Nombre de control según ISO/IEC 27002:2013
15.1.2	5.20	Abordar la seguridad en los acuerdos con los proveedores
15.1.3	5.21	Cadena de suministro de tecnología de la información y la comunicación
15.2		Gestión de entrega de servicios de proveedores
15.2.1	5.22	Seguimiento y revisión de servicios de proveedores
15.2.2	5.22	Gestión de cambios en los servicios del proveedor
dieciséis		Gestión de incidentes de seguridad de la información
16.1		Gestión de incidentes y mejoras de seguridad de la información
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Reportar eventos de seguridad de la información
16.1.3	6.8	Informar sobre debilidades en la seguridad de la información
16.1.4	5.25	Evaluación y decisión sobre eventos de seguridad de la información
16.1.5	5.26	Respuesta a incidentes de seguridad de la información
16.1.6	5.27	Aprender de los incidentes de seguridad de la información
16.1.7	5.28	Recolección de evidencia
17		Aspectos de seguridad de la información de la gestión de la continuidad del negocio
17.1		Continuidad de la seguridad de la información
17.1.1	5.29	Planificación de la continuidad de la seguridad de la información
17.1.2	5.29	Implementación de la continuidad de la seguridad de la información
17.1.3	5.29	Verificar, revisar y evaluar la continuidad de la seguridad de la información
17.2		despidos
17.2.1	8.14	Disponibilidad de instalaciones de procesamiento de información
18		Cumplimiento
18.1		Cumplimiento de requisitos legales y contractuales
18.1.1	5.31	Identificación de la legislación aplicable y requisitos contractuales
18.1.2	5.32	Derechos de propiedad intelectual
18.1.3	5.33	Protección de registros
18.1.4	5.34	Privacidad y protección de la información de identificación personal
18.1.5	5.31	Regulación de controles criptográficos
18.2		Revisiones de seguridad de la información
18.2.1	5.35	Revisión independiente de la seguridad de la información.
18.2.2	5.36	Cumplimiento de políticas y estándares de seguridad
18.2.3	5.36 ,8.8	Revisión de cumplimiento técnico

Bibliografía

[1]ISO 9000, *Sistemas de gestión de calidad - Fundamentos y vocabulario*

[2] ISO 55001, *Gestión de activos - Sistemas de gestión - Requisitos*

[3] ISO/IEC 11770 (todas las partes), *Seguridad de la información - Gestión de claves*

[4] ISO / IEC 15408 (todas las partes), *Tecnologías de la información - Técnicas de seguridad - Criterios de evaluación de seguridad informatica*

[5] ISO 15489 (todas las partes), *Información y documentación - Gestión de registros*

[6] ISO/IEC 17788, *Tecnología de la información - Computación en la nube - Descripción general y vocabulario*

[7] ISO/IEC 17789, *Tecnologías de la información - Computación en la nube - Arquitectura de referencia*

[8] ISO / IEC 19086 (todas las partes), *Informática en la nube: marco de acuerdo de nivel de servicio (SLA)*

[9] ISO / IEC 19770 (todas las partes), *Tecnología de la información - Gestión de activos de TI*

[10] ISO/IEC 19941, *Tecnologías de la información - Computación en la nube - Interoperabilidad y portabilidad*

[11] ISO/IEC 20889, *Terminología de desidentificación de datos que mejora la privacidad y clasificación de tecnicas*

[12] ISO 21500, *Gestión de proyectos, programas y portafolios - Contexto y conceptos*

[13] ISO 21502, *Gestión de proyectos, programas y carteras - Orientación sobre la gestión de proyectos*

[14] ISO 22301, *Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Requisitos*

[15] ISO 22313, *Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Orientación sobre el uso de ISO 22301*

[16] ISO/TS 22317, *Seguridad social - Sistemas de gestión de la continuidad del negocio - Directrices para el análisis de impacto empresarial (BIA)*

[17] ISO 22396, *Seguridad y resiliencia - Resiliencia comunitaria - Directrices para el intercambio de información entre organizaciones*

[18] ISO/IEC TS 23167, *Tecnología de la información - Computación en la nube - Tecnologías y técnicas comunes*

[19] ISO/IEC 23751: -2), *Tecnología de la información - Computación en la nube y plataformas distribuidas - Marco de acuerdo de intercambio de datos (DSA)*

[20] ISO/IEC 24760 (todas las partes), *Seguridad y privacidad de TI: un marco para la gestión de identidades*

[21] ISO/IEC 27001: 2013, *Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos*

[22] ISO/IEC 27005, *Tecnologías de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información*

[23] ISO/IEC 27007, *Seguridad de la información, ciberseguridad y protección de la privacidad - Directrices para auditoría de sistemas de gestión de seguridad de la información*

[24] ISO/IEC TS 27008, *Tecnologías de la información - Técnicas de seguridad - Directrices para la evaluación de los controles de seguridad de la información*

2) Durante la preparación. Etapa en el momento de la publicación: ISO/IEC PRF 23751:2022.

[25] ISO/IEC 27011, *Tecnologías de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para organizaciones de telecomunicaciones*

[26] ISO/IEC TR 27016, *Tecnologías de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Economía organizacional*

[27] ISO/IEC 27017, *Tecnologías de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube*

[28] ISO/IEC 27018, *Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII*

[29] ISO/IEC 27019, *Tecnología de la información - Técnicas de seguridad - Controles de seguridad de la información para la industria de servicios públicos de energía*

[30] ISO/IEC 27031, *Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la tecnología de la información y la comunicación para la continuidad del negocio*

[31] ISO/IEC 27033 (todas las partes), *Tecnologías de la información - Técnicas de seguridad - Seguridad en la red*

[32] ISO/IEC 27034 (todas las partes), *Tecnología de la información - Seguridad de aplicaciones*

[33] ISO/IEC 27035 (todas las partes), *Tecnologías de la información - Técnicas de seguridad - Seguridad de la información administracion de incidentes*

[34] ISO/IEC 27036 (todas las partes), *Tecnologías de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores*

[35] ISO/IEC 27037, *Tecnologías de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital*

[36] ISO/IEC 27040, *Tecnologías de la información - Técnicas de seguridad - Seguridad del almacenamiento*

[37] ISO/IEC 27050 (todas las partes), *Tecnología de la información - Descubrimiento electrónico*

[38] ISO/IEC TS 27110, *Tecnología de la información, ciberseguridad y protección de la privacidad: directrices para el desarrollo del marco de ciberseguridad*

[39] ISO/IEC 27701, *Técnicas de seguridad - Extensión a ISO/IEC 27001 e ISO/IEC 27002 para privacidad gestión de la información - Requisitos y lineamientos*

[40] ISO 27799, *Informática en salud - Gestión de la seguridad de la información en salud utilizando ISO/IEC 27002*

[41] ISO/IEC 29100, *Tecnologías de la información - Técnicas de seguridad - Marco de privacidad*

[42] ISO/IEC 29115, *Tecnología de la información - Técnicas de seguridad - Marco de garantía de autenticación de entidades*

[43] ISO/IEC 29134, *Tecnología de la información - Técnicas de seguridad - Directrices para la evaluación del impacto en la privacidad*

[44] ISO/IEC 29146, *Tecnología de la información - Técnicas de seguridad - Un marco para la gestión de acceso*

[45] ISO/IEC 29147, *Tecnologías de la información - Técnicas de seguridad - Divulgación de vulnerabilidades*

[46] ISO 30000, *Barcos y tecnología marina - Sistemas de gestión de reciclaje de barcos - Especificaciones para sistemas de gestión de instalaciones de reciclaje de buques seguras y respetuosas con el medio ambiente*

[47] ISO/IEC 30111, *Tecnologías de la información - Técnicas de seguridad - Procesos de manejo de vulnerabilidades*

[48] ISO 31000: 2018, *Gestión de riesgos - Directrices*

[49] CEI 31010, *Gestión de riesgos - Técnicas de evaluación de riesgos*

[50] ISO/IEC 22123 (todas las partes), *Tecnología de la información - Computación en la nube*

[51] ISO/IEC 27555, *Seguridad de la información, ciberseguridad y protección de la privacidad - Directrices sobre la eliminación de información de identificación personal*

[52] Foro de Seguridad de la Información (ISF). Estándar ISF de buenas prácticas para la seguridad de la información 2020, agosto de 2018. Disponible en https://www.securityforum.org/tool/standard-of - buenas-prácticas-para-la-seguridad-de-la-información-2020 /

[53] ITIL® Foundation, ITIL 4 edición, AXELOS, febrero de 2019, ISBN: 9780113316076

[54] Instituto Nacional de Estándares y Tecnología (NIST), SP 800-37, Marco de gestión de riesgos para sistemas y organizaciones de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad, revisión 2. Diciembre de 2018 [consultado el 31 de julio de 2020] . Disponible enhttps: // doi. org/10.6028/NIST.SP.800-37r2

[55] Proyecto de seguridad de aplicaciones web abiertas (OWASP). OWASP Top Ten - 2017, Los diez riesgos de seguridad de aplicaciones web más críticos, 2017 [consultado el 31 de julio de 2020]. Disponible enhttps: // avispa. org / www-project-top-ten / OWASP_Top_Ten_2017 /

[56] Proyecto de seguridad de aplicaciones web abiertas (OWASP). Guía para desarrolladores de OWASP, [en línea] [consultado el 22 de octubre de 2020]. Disponible enhttps://github.com/OWASP/DevGuide

[57] Instituto Nacional de Estándares y Tecnología (NIST), SP 800-63B, Pautas de identidad digital; Autenticación y Gestión del Ciclo de Vida. Febrero de 2020 [consultado el 31 de julio de 2020]. Disponible enhttps://doi.org/10.6028/NIST.SP.800-63b

[58] OASIS, Expresión estructurada de información sobre amenazas. Disponible enhttps://www.oasis-open.org/normas #stix2.0

[59] OASIS, Intercambio Automatizado Confiable de Información de Indicadores. Disponible enhttps: //www.oasis - open.org/standards#taxii2.0

ICS 35.030

Precio basado en 152 páginas