NORMA
CHILENA

NCh ISO/IEC 27002

Tercera edición
2022.12.27

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

Information security, cybersecurity and privacy protection — Information security controls

ICS 35.030

INSTITUTO NACIONAL DE NORMALIZACION

Número de referencia
NCh-ISO/IEC 27002:2022
195 páginas

DOCUMENTO PROTEGIDO POR COPYRIGHT

Instituto Nacional de Normalización - INN

Av. Libertador Bernardo O'Higgins 1449, Santiago Downtown Torre 7, piso 18 • Santiago de Chile

Tel. + 56 2 2445 88 00

Correo Electrónico contacto@inn.cl

Sitio Web www.inn.cl

Publicado en Chile

© ISO 2022 - Todos los derechos reservados
© INN 2022 - Para la adopción nacional

Contenido

Página

Tablas

Preámbulo

El Instituto Nacional de Normalización, INN, es el organismo que tiene a su cargo el estudio y preparación de las normas técnicas a nivel nacional. Es miembro de la INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) y de la COMISION PANAMERICANA DE NORMAS TECNICAS (COPANT), representando a Chile ante esos organismos.

Esta norma es una adopción idéntica de la versión en inglés/español de la Norma Internacional ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection - Information security controls*, y ha sido elaborada por el Instituto Nacional de Normalización para proporcionar un conjunto de referencia de controles genéricos de seguridad de la información que incluye una guía de implementación.

Para los propósitos de esta norma, se han realizado los cambios editoriales que se indican y justifican en Anexo D.

La Nota Explicativa incluida en un recuadro en Anexo C Bibliografía, es un cambio editorial que se incluye con el propósito de informar la equivalencia de las Normas Internacionales citadas en esta norma con las Normas Chilenas.

Los Anexos A, B, C y D no forman parte de la norma, se insertan solo a título informativo.

Esta norma reemplaza a la norma NCh-ISO 27002:2013 *Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información* y la deja no vigente técnicamente.

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 27 de diciembre de 2022.

Si bien se ha tomado todo el cuidado razonable en la preparación y revisión de los documentos normativos producto de la presente comercialización, INN no garantiza que el contenido del documento es actualizado o exacto o que el documento será adecuado para los fines esperados por el Cliente.

En la medida permitida por la legislación aplicable, el INN no es responsable de ningún daño directo, indirecto, punitivo, incidental, especial, consecuencial o cualquier daño que surja o esté conectado con el uso o el uso indebido de este documento.

0 Introducción

0.1 Antecedentes y contexto

Esta norma está diseñada para organizaciones de todo tipo y tamaño. Se usa 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) basada en la norma ISO/IEC 27001. También se puede usar como un documento de guía para las organizaciones que determinan e implementan controles de seguridad de información comúnmente aceptados. Además, esta norma está destinada a ser utilizada en desarrollo de directrices de gestión de seguridad de información específicas de industria y de organización, teniendo en cuenta su entorno de riesgo de seguridad de información específica. Se pueden determinar los controles específicos de la organización o de entorno distintos de los incluidos en esta norma mediante la evaluación de riesgos, según corresponda.

Las organizaciones de todo tipo y tamaño (incluyendo las del sector público privado comerciales y sin fines de lucro) crean, recogen, procesan, almacenan, transmiten y eliminan información en muchas formas, incluyendo 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 debería definir, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario. Un SGSI como el especificado en la norma ISO/IEC 27001 adopta una visión holística y coordinada de riesgos de seguridad de la información de la organización con el fin de determinar e implementar un conjunto completo de controles de seguridad de la información dentro del marco general de un sistema de gestión coherente.

Muchos sistemas de información, incluyendo gestión y operaciones, no se diseñaron para ser seguros en términos de un SGSI como se especifica en la norma ISO/IEC 27001 y en esta norma. El nivel de seguridad que se puede lograr solo a través de medidas tecnológicas es escaso y se deberían apoyar por actividades de gestión y procesos organizativos adecuados. La identificación de controles que deberían estar en su lugar requiere una planificación cuidadosa y la atención a detalles mientras se lleva a cabo el tratamiento de riesgos.

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

Un sistema de gestión de seguridad de la información apropiado 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. Existen tres fuentes principales de requisitos de seguridad de la información:

a) evaluación de riesgos para la organización, teniendo en cuenta la estrategia y objetivos empresariales generales de la organización. Esto se puede facilitar o apoyar a través de una evaluación de riesgos específica para seguridad de la información. Esto debería dar lugar a la determinación de controles necesarios para garantizar que el riesgo residual para la organización cumple con sus criterios de aceptación del riesgo;

b) requisitos legales, reglamentarios y contractuales que deberían cumplir una organización y sus partes interesadas (socios comerciales, proveedores de servicios, otros) y su entorno sociocultural;

c) conjunto de principios, objetivos y requisitos empresariales para todas las etapas del ciclo de vida de información que una organización desarrolló para apoyar sus operaciones.

0.3 Controles

Un control se define como una medida que modifica o mantiene el riesgo. Algunos de controles de esta norma son controles que modifican este, mientras que otros lo mantienen. Una política de seguridad de la información, por ejemplo, solo puede mantener el riesgo mientras que el cumplimiento de política de seguridad de la información puede modificar el riesgo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Esta norma proporciona una mezcla genérica de controles de seguridad de la información organizativos, humanos, 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 se deberían basar 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 debería 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 necesarios o identificarlos a partir de cualquier fuente. Al especificar dichos controles, la organización debería considerar recursos e inversión necesaria para implementar y operar un control contra el valor de negocio realizado. Ver norma ISO/IEC TR 27016 para obtener una Guía sobre las decisiones relativas a la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de requisitos de competencia de recursos.

Debería haber un equilibrio entre recursos desplegados para la implementación de controles y el potencial impacto empresarial resultante de incidentes de seguridad en ausencia de dichos controles. Resultados de una evaluación de riesgos deberían ayudar a orientar y determinar acciones de gestión apropiadas, prioridades para gestión de riesgos de seguridad de la información y para la implementar controles que se determinen necesarios para proteger contra estos riesgos.

Algunos de los controles de esta norma se pueden considerar como principios rectores de gestión de seguridad de la información y aplicables a la mayoría de las organizaciones. En la norma ISO/IEC 27005 se puede encontrar más información sobre la determinación de controles y otras opciones de tratamiento del riesgo.

0.5 Elaboración de directrices específicas para la organización

Esta norma se puede considerar un punto de partida para desarrollar directrices específicas para la organización. No todos los controles y directrices de esta norma se pueden aplicar a todas las organizaciones. También se pueden requerir controles y directrices adicionales no incluyendo en esta norma para abordar necesidades específicas de la organización y riesgos que se identificaron. En que se desarrollen documentos que contengan directrices o controles adicionales, puede ser útil incluir referencias cruzadas a cláusulas de esta norma para futuras referencias.

0.6 Consideraciones sobre el ciclo de vida

La información tiene un ciclo de vida, desde su creación hasta su eliminación. El valor y riesgos de información pueden variar a lo largo de este ciclo de vida (por ejemplo, divulgación no autorizada o el robo de cuentas financieras de una empresa no son significativos después de su publicación, pero la integridad sigue siendo fundamental), porque la seguridad de la información sigue siendo importante en cierta medida en todas las etapas.

Los sistemas de información y otros activos relevantes para seguridad de la información tienen ciclos de vida dentro de los cuales se conciben, especifican, diseñan, desarrollan, prueban, implementan, usan, mantienen y eventualmente se retiran del servicio y se eliminan. Se debería tomar en cuenta la seguridad de información en todas las etapas. Los proyectos de desarrollo de nuevos sistemas y cambios en sistemas existentes ofrecen oportunidades para mejorar controles de seguridad, teniendo en cuenta riesgos de la organización y las lecciones aprendidas a partir de incidentes.

0.7 Norma Internacional sobre Servicios Relacionados

Mientras que esta norma ofrece una guía sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones diferentes, otros documentos de las normas ISO/IEC 27000 proporcionan asesoramiento o requisitos complementarios sobre otros aspectos del proceso general de gestión de seguridad de la información.

Consultar norma ISO/IEC 27000 para obtener una introducción general al SGSI y a la familia de documentos. ISO/IEC 27000 proporciona un glosario que define la mayoría de los términos usados en la familia de documentos ISO/IEC 27000 y describe el alcance y campo de aplicación y objetivos de cada miembro de la familia.

Hay normas específicas del sector que tienen controles adicionales que pretenden abordar áreas específicas (por ejemplo, ISO/IEC 27017 para servicios en la nube, ISO/IEC 27701 para la privacidad, ISO/IEC 27019 para la energía, ISO/IEC 27011 para las organizaciones de telecomunicaciones e ISO 27799 para la salud). Dichas normas se incluyen en la bibliografía y algunas de ellas se mencionan en secciones de Guía y otra información de cláusulas 5 a 8.

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

1 Alcance y campo de aplicación

Esta norma proporciona un conjunto de referencia de controles genéricos de seguridad de la información que incluye una guía de implementación. Esta norma está diseñada para ser usada por las organizaciones:

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

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

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

2 Referencias normativas

No hay referencias normativas.

3 Términos y definiciones

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

ISO e IEC mantienen bases terminológicas que se pueden utilizar para normalización en las siguientes direcciones:

— Plataforma en línea de ISO: disponible en https://www.iso.org/obp

— IEC Electropedia: disponible en https://www.electropedia.org

3.1 Términos y definiciones

3.1.1
control de acceso
medios para garantizar que el acceso físico y lógico a activos (ver 3.1.2) esté autorizado y restringido en función de requisitos de seguridad de la empresa y de información

3.1.2
activo
cualquier cosa que tenga valor para la organización

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

— activos principales:

  — información;

  — procesos empresariales (ver 3.1.27) y actividades;

— Los activos de apoyo (de que dependen activos primarios) de todo tipo, por ejemplo:

  — hardware;

  — software;

  — red;

  — personal (ver 3.1.20);

  — sitio;

  — estructura de la organización.

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

3.1.4
autenticación
proporcionar garantías de que una característica declarada de una entidad (ver 3.1.11) es correcta

3.1.5
autenticidad
propiedad de que una entidad (ver 3.1.11) es que dice ser

3.1.6
cadena de custodia
posesión, movimiento manipulación y ubicación demostrables de material desde un momento hasta otro

Nota 1 a la entrada: Material incluye información y otros activos asociados (3.1.2) en el contexto de la norma 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 se pretende poner a disposición o divulgar a personas, entidades (ver 3.1.11) o procesos no autorizados (ver 3.1.27)

3.1.8
control
medida que mantiene y/o modifica el riesgo

Nota 1 a la entrada: Controles incluyen, sin limitaciones a, cualquier proceso (ver 3.1.27), política (ver 3.1.24), dispositivo práctico u otras condiciones y/o acciones que mantienen y/o modifican el riesgo.

Nota 2 a la entrada: Controles pueden no ejercer siempre el efecto modificador previsto o supuesto.

[FUENTE: ISO 31000:2018, 3.8]

3.1.9
perturbación
incidente, previsto o imprevisto que provoca una desviación negativa y no planificada de la entrega prevista de productos y servicios de acuerdo con objetivos de una organización

[FUENTE: ISO 22301:2019, 3.10]

3.1.10
dispositivo terminal
dispositivo de hardware de tecnología de información y comunicaciones (TIC) conectado a la red

Nota 1 a la entrada: El dispositivo terminal se puede referir a computadores de sobremesa, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, impresoras u otro hardware especializado incluyendo contadores inteligentes y dispositivos del internet de las cosas (IoT).

3.1.11
entidad
elemento relevante para el funcionamiento de un dominio que tiene una existencia reconociblemente distinta

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

EJEMPLO Una persona, una organización, un dispositivo un grupo de tales elementos, un abonado humano a un servicio de telecomunicaciones, 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 de tratamiento de información, servicio o infraestructura, o la ubicación física que lo alberga

[FUENTE: ISO/IEC 27000:2018, 3.27, modificado “instalaciones” se sustituyó por instalación.]

3.1.13
violación de seguridad de la información
compromiso de seguridad de la información que conduzca a destrucción no deseada, pérdida, alteración, divulgación o el acceso a información protegida transmitida, almacenada o procesada de otro modo

3.1.14
evento de seguridad de la información
suceso que indique una posible violación de seguridad de la información (ver 3.1.13) o un fallo de controles (ver 3.1.8)

[FUENTE: ISO/IEC 27035-1:2016, 3.3, modificado “violación de seguridad de la información” se sustituyó por “violación de seguridad de la información”.]

3.1.15
incidente de seguridad de la información
uno o varios eventos de seguridad de la información relacionados e identificados (ver 3.1.14) que pueden dañar activos de una organización (ver 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 coherente y eficaz para gestión de incidentes de seguridad de la información (ver 3.1.15)

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

3.1.17
sistema de información
conjunto de aplicaciones, servicios, activos de tecnología de información (ver 3.1.2) u otros componentes de tratamiento de información

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

3.1.18
parte interesada
persona u organización que puede afectar, verse afectada o percibir que se ve afectada por una decisión o actividad

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

3.1.19
no repudio
capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen (ver 3.1.11)

3.1.20
personal
personas que realizan trabajos bajo dirección de la organización

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

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

Nota 1 a la entrada: La “persona física” en la definición es el titular de PII (ver 3.1.22). Para determinar si el titular de PII es identificable, se deberían tener en cuenta todos los medios que razonablemente se puedan usar por el interesado en protección de la intimidad que posee los datos o por 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
principal PII
persona física a la que se refiere Información de identificación personal (PII) (ver 3.1.21)

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

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

3.1.23
procesador PII
parte interesada en la privacidad que procesa información de identificación personal (PII) (ver 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 del impacto sobre la privacidad
PIA
proceso global (ver 3.1.27) de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de los posibles impactos sobre la privacidad en relación con el tratamiento de Información de identificación personal (PII) (ver 3.1.21), enmarcado con el 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 especificada de llevar a cabo una actividad o un proceso (ver 3.1.27)

[FUENTE: ISO 30000:2009, 3.12]

3.1.27
proceso
conjunto de actividades interrelacionadas o que interactúan entre sí y que usan o transforman los insumos para obtener un resultado

[FUENTE: ISO 9000:2015, 3.4.1, modificado Notas de entrada eliminadas.]

3.1.28
registro
información creada, recibida y conservada como prueba y activo (ver 3.1.2) por una organización o persona, en cumplimiento de obligaciones legales o en realización de negocios

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

[FUENTE: ISO 15489-1:2016, 3.14, modificado “Nota 1 a la entrada” añadida].

3.1.29
objetivo de punto de recuperación
RPO
punto en el tiempo al que se deberían recuperar los datos tras tener una interrupción (ver 3.1.9)

[FUENTE: ISO/IEC 27031:2011, 3.12, modificado “deberían” se sustituye por “deberían ser”.]

3.1.30
tiempo de recuperación del objetivo
RTO
período en que se deberían recuperar niveles mínimos de servicios y/o productos y sistemas, aplicaciones o funciones de apoyo después de que se produzca una interrupción (ver 3.1.9)

[FUENTE: ISO/IEC 27031:2011, 3.13, modificado “deberían” se sustituye por “deberían ser”]

3.1.31
fiabilidad
propiedad de comportamiento y resultados previstos coherentes

3.1.32
regla
principio o instrucción aceptada que establece las expectativas de la organización sobre que se debería hacer, que está permitido o no

Nota 1 a la entrada: Las Reglas se pueden expresar formalmente en políticas específicas por temas (ver 3.1.35) y en otros tipos de documentos.

3.1.33
información confidencial
información que se debería proteger de la no disponibilidad, acceso no autorizado modificación o divulgación pública debido a los posibles efectos adversos para una persona, una organización, seguridad nacional o pública

3.1.34
amenaza
causa potencial de un incidente no deseado que puede provocar daños en 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 asunto específico expresadas formalmente por el nivel apropiado de dirección

Nota 1 a la entrada: Políticas específicas de tema pueden expresar formalmente reglas (ver 3.1.32) o normas de la organización.

Nota 2 a la entrada: Algunas organizaciones usan otros términos para estas políticas específicas del tema.

Nota 3 a la entrada: Políticas específicas de tema a que se refiere esta norma están relacionadas con seguridad de la información.

EJEMPLO Política específica de temas obre control de acceso (ver 3.1.1), política específica de tema sobre escritorio y pantalla claros.

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

EJEMPLO Personal (ver 3.1.20), clientes, proveedores.

3.1.37
dispositivo terminal del usuario
dispositivo terminal (ver 3.1.10) utilizado por usuarios para acceder a servicios de tratamiento de información

Nota 1 a la entrada: El dispositivo terminal del usuario se puede referir a computadores de sobremesa, portátiles, teléfonos inteligentes, tabletas, clientes ligeros, otro.

3.1.38
vulnerabilidad
debilidad de un activo (ver 3.1.2) o de un control (ver 3.1.8) que se puede aprovechar por una o más amenazas (ver 3.1.34)

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

3.2 Términos abreviados

ABAC	control de acceso basado en atributos
ACL	lista de control de acceso
BIA	análisis del impacto empresarial
BYOD	trae tu propio dispositivo
CAPTCHA	test de Turing público y automático para distinguir a los computadores de los humanos
CPU	unidad central de procesamiento
DAC	control de acceso discrecional
DNS	sistema de nombres de dominio

GPS	sistema de posicionamiento global
IAM	gestión de identidades y accesos
ICT	tecnología de información y la comunicación
ID	identificador
IDE	entorno de desarrollo integrado
IDS	sistema de detección de intrusos
IoT	internet de las cosas
IP	protocolo de internet
IPS	sistema de prevención de intrusiones
TI	tecnología de información
SGSI	sistema de gestión de seguridad de la información
MAC	control de acceso obligatorio
NTP	protocolo de tiempo de red
PIA	evaluación de impacto sobre la privacidad
PII	información de identificación personal
PIN	número de identificación a 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	tiempo de recuperación del objetivo
SAST	pruebas de seguridad de aplicaciones estáticas
SD	digital seguro
SDN	redes definidas por software
SD-WAN	red de área amplia definida por software
SIEM	gestión de información y eventos de seguridad
SMS	servicio de mensajes cortos

SQL	lenguaje de consulta estructurado
SSO	inicio de sesión único
SWID	identificación del software
UEBA	análisis de comportamiento de usuarios y entidades
SAI	sistema de alimentación ininterrumpida
URL	localizador uniforme de recursos
USB	bus serial universal
VM	máquina virtual
VPN	red privada virtual
WiFi	fidelidad inalámbrica

4 Estructura de esta norma

4.1 Cláusulas

Esta norma está estructurada de la manera siguiente:

a) Controles organizativos (ver cláusula 5)

b) Controles de personas (ver cláusula 6)

c) Controles físicos (ver cláusula 7)

d) Controles tecnológicos (ver cláusula 8)

Hay 2 anexos informativos:

Anexo A Uso de atributos

Anexo B Relación con ISO/IEC 27002:2013

El Anexo A explica cómo una organización puede usar atributos (ver 4.2) para crear sus propias vistas basadas en atributos de control definidos en esta norma o de su propia creación.

El Anexo B muestra la relación entre controles de esta edición de la norma ISO/IEC 27002 y la anterior edición de 2013.

4.2 Temas y atributos

La categorización de controles que figuran en cláusulas 5 a 8 se denomina temas. Los controles se clasifican como:

a) personas, si se trata de personas individuales;

b) físicas, si se refieren a objetos físicos;

c) tecnológicos, si se refieren a la tecnología;

d) en caso contrario se clasifican como organizativas.

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 públicos. El Anexo A explica cómo se puede lograr esto y proporciona un ejemplo de una vista.

A modo de ejemplo a cada control de esta norma se le han asociado cinco atributos con sus correspondientes valores de atributo (precedidos de "#" para que se puedan buscar), como sigue:

a) Tipo de control

Tipo de control es un atributo para ver 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 del atributo consisten en Preventivo (el control que pretende prevenir la ocurrencia de un incidente de seguridad de la información), de detección (el control actúa cuando ocurre un incidente de seguridad de la información) y Correctivo (el control actúa después de que ocurra un incidente de seguridad de la información).

b) Propiedades de seguridad de la información

Propiedades de seguridad de la información es un atributo para ver controles desde la perspectiva de qué característica de información contribuirá a preservar el control. Los valores del atributo consisten en confidencialidad, integridad y disponibilidad.

c) Conceptos de ciberseguridad

Conceptos de ciberseguridad es un atributo para ver controles desde la perspectiva de la asociación de controles a conceptos de ciberseguridad definidos en el marco de ciberseguridad descrito en ISO/IEC TS 27110. Valores del atributo consisten en identificar, proteger, detectar, responder y recuperar.

d) Capacidades operativas

Capacidades operativas es un atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Valores de atributos consisten en gobernanza, Gestión de activos, Information_protection, Human_resource_security, Physical_security, System_and_network_security, Application_security, Secure_configuration, Identity_and_access_management, Threat_and_vulnerability_management, Continuit, Supplier_relationships_security, Legal_and_compliance, Information_security_event_management y Information_security_assurance.

e) Dominios de seguridad

Dominios de seguridad es un atributo para ver controles desde la perspectiva de cuatro dominios de seguridad de la información: Governance and Ecosystem incluyendo Information System Security Governance & Risk Management y Ecosystem cybersecurity management (incluyendo a partes interesadas internas y externas partes interesadas); Protection incluyendo IT Security Architecture, IT Security Administration, Identity and access management, IT Security Maintenance y Physical and environmental security; Defence incluyendo Detection y Computer Security Incident Management; Resilience incluyendo Continuity of operations y Crisis management. Valores de atributos son Governance_and_Ecosystem, Protection, Defence y Resilience.

Se seleccionaron estos atributos indicados en esta norma, porque se consideran lo bastante genéricos como para ser utilizado por diferentes tipos de organizaciones. Las organizaciones pueden optar por prescindir de uno o varios de atributos indicados en esta norma. También pueden crear atributos propios (con los valores de atributo correspondientes) para crear sus propias vistas organizativas. A.2 incluye ejemplos de dichos atributos.

4.3 Control diseño

El diseño de cada control contiene lo siguiente:

— **Título del control**: Nombre corto del control;

— **Tabla de atributos**: Una tabla muestra el o los valores de cada atributo para el control dado;

— **Control**: Qué es el control;

— **Propósito**: Por qué se debería implementar el control;

— **Guía**: Cómo se debería aplicar el control;

— **Otros Datos**: Texto explicativo o referencias a otros documentos relacionados.

Se usan subtítulos en el texto de las orientaciones para facilitar la lectura en que las orientaciones son extensas y abordan varios temas. Estos títulos no se usan necesariamente en todo el texto de las orientaciones. Subtítulos están subrayados.

5 Controles organizativos

5.1 Políticas de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Política de seguridad de la información y políticas específicas de cada tema se deberían definir, aprobadas por dirección, publicadas, comunicadas y reconocidas por personal y partes interesadas pertinentes, revisadas a intervalos planificados y si se producen cambios significativos.

Propósito

Garantizar la idoneidad, adecuación y eficacia continuas de dirección y apoyo a seguridad de la información de acuerdo con requisitos empresariales, legales, reglamentarias y contractuales.

Guía

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

La política de seguridad de la información debería tener en cuenta requisitos derivados de:

a) estrategia y requisitos de la empresa;

b) normativa, la legislación y contratos;

c) los riesgos y amenazas de seguridad de la información actual y proyectada;

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

a) definición de seguridad de la información;

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

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

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

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

f) asignación de responsabilidades para gestión de seguridad de la información a funciones definidas;

g) procedimientos de gestión de extensiones y excepciones.

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

En un nivel inferior, la política de seguridad de la información debería estar respaldada por políticas específicas por temas, según sea necesario para ordenar aplicación de controles de seguridad de la información. Las políticas de temas específicos suelen estar estructuradas para responder a necesidades de determinados grupos dentro de una organización o para cubrir ciertas áreas de seguridad. Las políticas temáticas deberían estar alineadas con política de seguridad de la información de la organización y complementarla.

Algunos ejemplos de estos temas son:

a) control de acceso;

b) seguridad física y medioambiental;

c) gestión de activos;

d) transferencia de información;

e) configuración y manejo seguros de los dispositivos de usuarios;

f) seguridad en la red;

g) gestión de incidentes de seguridad de la información;

h) copia de seguridad;

i) criptografía y gestión de claves;

j) clasificación y tratamiento de información;

k) gestión de las vulnerabilidades técnicas;

l) desarrollo seguro.

La responsabilidad de la elaboración, revisión y aprobación de políticas específicas de cada tema se debería asignar al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica. Revisión debería incluir evaluación de oportunidades de mejora de política de seguridad de la información de la organización y de políticas específicas de tema y gestión de seguridad de la información en respuesta a cambios:

a) la estrategia empresarial de la organización;

b) el entorno técnico de la organización;

c) reglamentos, estatutos, legislación y contratos;

d) riesgos para seguridad de la información;

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

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

La revisión de política de seguridad de la información y de políticas de temas específicos debería tener en cuenta resultados de revisiones y auditorías de dirección. Revisión y actualización de otras políticas relacionadas se debería considerar cuando se modifique una política para mantener la coherencia.

La política de seguridad de la información y políticas específicas de cada tema se deberían comunicar a personal y a partes interesadas de una forma que sea pertinente, accesible y comprensible para el lector previsto. A los destinatarios de políticas se les debería pedir que reconozcan que las entienden y que se comprometen a cumplirlas, cuando corresponda. La organización puede determinar los formatos y nombres de estos documentos de política que satisfagan necesidades de la organización. En algunas organizaciones, política de seguridad de la información y políticas de temas específicos pueden estar en un solo documento. La organización puede denominar estas políticas específicas por temas como normas, directivas, políticas u otros.

Si la política de seguridad de la información o cualquier política específica de un tema se distribuyen fuera de la organización, se debe poner especial atención de no revelar información confidencial de manera inapropiada.

La Tabla 1 ilustra las diferencias entre política de seguridad de la información y política temática.

Tabla 1 – Diferencias entre política de seguridad de la información y política temática

	Política de seguridad de la información	Política específica del tema
Nivel de detalle	General o de alto nivel	Específicos y detallados
Documentado y aprobado formalmente por	Alta dirección	Nivel de gestión adecuado

Otra información

Las políticas específicas de cada tema pueden variar según las organizaciones.

5.2 Funciones y responsabilidades de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Las funciones y responsabilidades de seguridad de la información se deberían definir y asignar en función de necesidades de la organización.

Propósito

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

Guía

Asignación de funciones y responsabilidades en materia de seguridad de la información se debería hacer de acuerdo con política de seguridad de la información y políticas específicas de cada tema (ver 5.1). La organización debería definir y gestionar las responsabilidades de:

a) protección de información y otros activos asociados;

b) realización de 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, a propietarios de riesgos);

d) uso información de una organización y otros activos asociados de todo personal.

Estas responsabilidades se deberían complementar, 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 deberían determinar que las tareas delegadas se hayan realizado correctamente.

Cada área de seguridad de la que son responsables individuos se debería definir, documentar y comunicar. Los niveles de autorización se deberían definir y documentar. Las personas que asumen una función específica de seguridad de la información deberían ser competentes en el conocimiento y las habilidades requeridas por la función y deberían recibir apoyo para mantener al día los desarrollos relacionados con la función y necesarios para cumplir con las responsabilidades de la función.

Otra información

Muchas organizaciones nombran a un responsable de seguridad de la información para que asuma responsabilidad general de desarrollo e aplicación de seguridad de la información y apoye la identificación de riesgos y controles de mitigación.

Sin embargo, responsabilidad de dotar de recursos y aplicar controles suele recaer en gestores individuales. Una práctica habitual es designar a un propietario para cada activo que se hace responsable de su protección diaria.

Dependiendo del tamaño y de los recursos de una organización, la seguridad de la información puede estar cubierta por funciones específicas o por funciones adicionales a existentes.

5.3 Segregación de funciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Gobernance #Identity_and_access_ management	#Governance_and_Ecosystem

Control

Funciones y áreas de responsabilidad conflictivas deberían estar separadas.

Propósito

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

Guía

Segregación de funciones y áreas de responsabilidad tiene como objetivo separar funciones conflictivas entre diferentes personas para evitar que una persona ejecute por sí misma posibles funciones conflictivas.

La organización debería determinar qué funciones y áreas de responsabilidad se deberían segregar. Los siguientes son ejemplos de actividades que pueden requerir segregación:

a) iniciar, aprobar y ejecutar un cambio;

b) solicitar, aprobar y aplicar los derechos de acceso;

c) diseñar, implementar y revisar el código;

d) desarrollar software y administración de sistemas de producción;

e) usar y administrar las aplicaciones;

f) usar aplicaciones y administrar bases de datos;

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

Se debería 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 se debería aplicar en la medida de lo posible y practicable. Siempre que sea difícil segregar, se deberían considerar otros controles, como el monitoreo de las actividades, las pistas de auditoría y la supervisión de la gestión.

Se debería poner especial atención 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 debería considerar el uso de herramientas automatizadas para identificar conflictos y facilitar su eliminación. Los roles se deberían definir y aprovisionar cuidadosamente para minimizar los problemas de acceso si se elimina o reasigna un rol.

Otra información

Sin información.

5.4 Responsabilidades de gestión

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

Control

La dirección debería exigir a todo personal que aplique seguridad de la información de acuerdo con política de seguridad de la información establecida, políticas y procedimientos específicos de la organización.

Propósito

Garantizar que la dirección entiende su papel en seguridad de la información y emprender acciones destinadas a garantizar que todo personal es consciente de sus responsabilidades en materia de seguridad de la información y las cumple.

Guía

La dirección debería demostrar su apoyo a política de seguridad de la información, a políticas específicas, a procedimientos y a controles de seguridad de la información.

Entre las responsabilidades de la dirección deberían incluir la garantía de que el personal:

a) esté debidamente informados de sus funciones y responsabilidades en materia de seguridad de la información antes de que se le conceda acceso a información de la organización y a otros activos asociados;

b) proporcione directrices que establecen las expectativas de seguridad de la información de su función dentro de la organización;

c) tenga mandato de cumplir política de seguridad de la información y políticas específicas de la organización;

d) alcance un nivel de concientización sobre seguridad de la información pertinente para sus funciones y responsabilidades dentro de la organización (ver 6.3);

e) cumpla las condiciones de empleo contrato o acuerdo incluida política de seguridad de la información de la organización y los métodos de trabajo adecuados;

f) siga disponiendo de las competencias y cualificaciones adecuadas en materia de seguridad de la información mediante una formación profesional continua;

g) disponga de un canal confidencial para denunciar las violaciones de política de seguridad de la información, en que sea posible, de políticas o procedimientos específicos de seguridad de la información (whistleblowing). Esto puede permitir una denuncia anónima, o tener disposiciones que garanticen que el conocimiento de la identidad del denunciante es conocido solo por aquel que necesitan tratar dichos informes;

h) proporcione recursos adecuados y el tiempo de planificación del proyecto para implantar procesos y controles relacionados con seguridad de la organización.

Otra información

Sin información.

5.5 Contacto con autoridades

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Correctivo	#Confidentiality #Integrity #Availability	#Identify #Protect #Responder #Recuperar	#Governance	#Defence #Resilience

Control

La organización debería establecer y mantener el contacto con autoridades pertinentes.

Propósito

Garantizar un flujo de información adecuado con respecto a seguridad de la información entre la organización y autoridades legales, reglamentarias y de supervisión pertinentes.

Guía

La organización debería especificar cuándo y quién se debería poner en contacto con autoridades (por ejemplo, fuerzas de seguridad, organismos reguladores, autoridades de supervisión) y cómo se deberían notificar oportunamente incidentes de seguridad de la información identificados.

También se deberían usar contactos con autoridades para facilitar la comprensión de las expectativas actuales y futuras de estas autoridades (por ejemplo, normas de seguridad de la información aplicables).

Otra información

Organizaciones atacadas pueden solicitar a autoridades que actúen contra la fuente del ataque.

Mantener estos contactos puede ser un requisito para apoyar gestión de incidentes de seguridad de la información (ver 5.24 a 5.28) o procesos de planificación de contingencia y continuidad del negocio (ver 5.29 y 5.30). Contactos con los organismos reguladores también son útiles para anticipar y preparar para los próximos cambios en las leyes o reglamentos pertinentes que afectan a la organización. Contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, proveedores de electricidad, salud y seguridad [por ejemplo, departamentos de bomberos (en relación con la continuidad del negocio), proveedores de telecomunicaciones (en relación con el enrutamiento y disponibilidad de líneas) y proveedores de agua (en relación con instalaciones de refrigeración de los equipos)].

5.6 Contacto con grupos de interés especial

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Correctivo	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defensa

Control

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

Propósito

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

Guía

Ser miembro de grupos o foros de interés especial, se debería considerar como un medio para:

a) mejorar los conocimientos sobre las mejores prácticas y mantener al día información de seguridad pertinente;

b) garantizar que la comprensión del entorno de seguridad de la información está actualizada;

c) recibir avisos tempranos de alertas, avisos y parches relativos a ataques y vulnerabilidades;

d) acceder a un asesoramiento especializado en materia de 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 trate de incidentes de seguridad de la información (ver los puntos 5.24 a 5.28).

Otra información

Sin información.

5.7 Inteligencia de amenazas

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detectar #Responder	#Threat_and_vulnerability_management	#Defence #Resilience

Control

La información relacionada con las amenazas a la seguridad de la información se debería recopilar y analizar para generar inteligencia de amenazas.

Propósito

Proporcionar conocimiento del entorno de amenazas de la organización para que se puedan tomar las acciones de mitigación apropiadas.

Guía

Información sobre amenazas existentes o emergentes se recoge y analiza con el fin de:

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

b) reducir el impacto de dichas amenazas.

La información sobre amenazas se puede dividir en tres niveles, que se deberían considerar:

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

b) inteligencia táctica sobre amenazas: información sobre metodologías, herramientas y tecnologías de los atacantes;

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

La información sobre amenazas debería ser:

a) pertinente (por ejemplo, relacionado con protección de la organización);

b) perspicaz (por ejemplo, que proporcione a la organización un conocimiento preciso y detallado del panorama de amenazas);

c) contextual, para proporcionar conocimiento de la situación (por ejemplo, añadir contexto a información en función del momento en que se producen los acontecimientos, lugar en que se producen, experiencias anteriores y prevalencia en organizaciones similares);

d) procesable (por ejemplo, que la organización pueda actuar sobre información de forma rápida y eficaz).

Las actividades de inteligencia de amenazas deberían incluir:

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

b) identificación, examen y selección de las fuentes de información internas y externas que sean necesarias y adecuadas para proporcionar información requerida para la producción de inteligencia sobre amenazas;

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

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

e) análisis de información para entender cómo se relaciona y tiene sentido para la organización;

f) comunicación con personas pertinentes en un formato que se pueda comprender.

La información sobre amenazas posteriormente se debería analizar y usar:

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

b) como aportación adicional a controles técnicos preventivos y de detección, como cortafuegos, sistemas de detección de intrusos o soluciones antimalware;

c) como aportación a procesos y técnicas de pruebas de seguridad de la información.

La organización debería compartir información sobre amenazas con otras organizaciones de forma mutua para mejorar información general sobre amenazas.

Otra información

Organizaciones pueden usar la inteligencia sobre amenazas para prevenir, detectar o responder a las mismas. Organizaciones pueden producir inteligencia sobre amenazas, pero lo más habitual es que reciban y usen la inteligencia sobre amenazas producida por otras fuentes.

La inteligencia sobre amenazas se suele proporcionar por proveedores o asesores independientes, agencias gubernamentales o grupos de inteligencia sobre amenazas en colaboración.

La eficacia de controles, como 5.25, 8.7, 8.16 u 8.23, depende de la calidad de información disponible sobre amenazas.

5.8 Seguridad de información en gestión de proyectos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection

Control

La seguridad de información se debería integrar en gestión del proyecto.

Propósito

Garantizar que riesgos de seguridad de la información relacionados con proyectos y resultados se abordan de forma eficaz en gestión de proyectos a lo largo del ciclo de vida de estos.

Guía

Se debería integrar la seguridad de información en gestión del proyecto para garantizar que riesgos de seguridad de la información se abordan como parte de 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 empresarial básico ICT, gestión de instalaciones u otros procesos de apoyo).

La gestión de proyectos en uso debería exigir que:

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

b) requisitos de seguridad de la información [por ejemplo, requisitos de seguridad de las aplicaciones (8.26), requisitos de cumplimiento de los derechos de propiedad intelectual (5.32), otro] se abordan en las primeras fases de proyectos;

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

d) avances en el tratamiento de riesgos para seguridad de la información se revisan, se evalúa y comprueba la eficacia del tratamiento.

La idoneidad de las consideraciones y actividades en materia de seguridad de la información debería ser objeto de monitoreo en fases predefinidas por personas u órganos de gobierno adecuados, como el comité de dirección del proyecto.

Las responsabilidades y autoridades en materia de seguridad de la información relevantes para el proyecto se deberían definir y asignar a roles específicos.

Los requisitos de seguridad de la información para los productos o servicios que entregará el proyecto se deberían determinar 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 se deberían determinar para todos los tipos de proyectos, no solo para los proyectos de desarrollo de TIC. También se debería considerar lo siguiente al determinar estos requisitos:

a) de qué información se trata (determinación de información), cuáles son necesidades correspondientes en materia de seguridad de la información (clasificación; ver 5.12) y las posibles repercusiones negativas para la empresa que se pueden derivar de la falta de seguridad adecuada;

b) necesidades de protección de información y otros activos asociados implicados, especialmente en términos de confidencialidad, integridad y disponibilidad;

c) el nivel de confianza o de garantía requerido respecto a la identidad declarada de las entidades para derivar requisitos de autenticación;

d) procesos de provisión y autorización de acceso para los clientes y otros usuarios potenciales de la empresa, así como para usuarios privilegiados o técnicos, como los miembros pertinentes del proyecto personal potencial de operaciones o proveedores externos;

e) información a usuarios de sus obligaciones y responsabilidades;

f) requisitos derivados de procesos empresariales, como el registro y supervisión de las transacciones, requisitos de no repudio;

g) requisitos exigidos por otros controles de seguridad de la información (por ejemplo, las interfaces con sistemas de registro y supervisión o de detección de fugas de datos);

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

i) nivel de confianza o garantía requerido para que los terceros cumplan política de seguridad de la información de la organización y políticas específicas del tema, incluyendo cláusulas de seguridad pertinentes en cualquier acuerdo o contrato.

Otra información

El enfoque de desarrollo del proyecto como el ciclo de vida en cascada o ciclo de vida ágil, debería apoyar seguridad de la información de una manera estructurada que se pueda adaptar a la gravedad evaluada de riesgos de seguridad de la información, según el carácter del proyecto. La consideración temprana de requisitos de seguridad de la información para el producto o servicio (por ejemplo, en las fases de planificación y diseño), puede conducir a soluciones más eficaces y rentables para la calidad y seguridad de la información. Las normas ISO 21500 e ISO 21502 ofrecen guías sobre conceptos y procesos de gestión de proyectos que son importantes para realización de estos.

La norma ISO/IEC 27005 orienta sobre uso de procesos de gestión de riesgos para identificar controles para cumplir con requisitos de seguridad de la información.

5.9 Inventario de información y otros activos asociados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Control

Se debería elaborar y mantener un inventario de información y otros activos asociados, incluyendo propietarios.

Propósito

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

Guía

Inventario

La organización debería identificar su información, otros activos asociados y determinar su importancia en términos de seguridad de la información. La documentación se debería mantener en inventarios específicos o existentes, según corresponda.

El inventario de información y otros activos asociados se debería precisar, estar actualizado, ser coherente y estar alineado con otros inventarios. Las opciones para garantizar la exactitud de un inventario de información y otros activos asociados incluyen:

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

b) aplicar automáticamente una actualización del inventario en el proceso de instalación, modificación o eliminación de un bien.

La ubicación de un activo se debería incluir en el inventario según corresponda.

El inventario no tiene por qué ser una lista única de información y otros activos asociados. Teniendo en cuenta que el inventario se debería mantener por funciones pertinentes, se puede ver como un conjunto de inventarios dinámicos, como inventarios de activos de información, hardware, software, máquinas virtuales (VM), instalaciones, a personal, competencia, capacidades y registros.

Cada activo se debería clasificar de acuerdo con clasificación de información (ver 5.12) asociada a ese activo.

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

Propiedad

Para información identificada y otros activos asociados, la propiedad del activo se debería asignar a un individuo o a un grupo y la clasificación se debería identificar (ver 5.12, 5.13). Se debería implementar un proceso que garantice la asignación oportuna de propiedad de activos. La propiedad se debería asignar cuando se crean activos o cuando se transfieren a la organización. La propiedad de activos se debería reasignar según sea necesario cuando propietarios actuales de activos se vayan o cambien de función.

Funciones del propietario

El propietario de un activo se debería responsabilizar de su correcta gestión a lo largo de todo su ciclo de vida, garantizando lo siguiente:

a) información inventariada y otros activos asociados;

b) información y otros activos asociados están apropiadamente clasificados y protegidos;

c) clasificación se revisa periódicamente;

d) enumeración y vinculación de componentes que soportan activos tecnológicos, como base de datos, almacenamiento componentes y subcomponentes de software;

e) requerimientos para el uso aceptable de información y otros activos asociados (ver 5.10) se establece;

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

g) información y otros activos asociados, cuando se borran o eliminan, se tratan de forma segura y se eliminan del inventario;

h) participación en la identificación y gestión de riesgos asociados a sus activos;

i) prestación de apoyo a personal que tiene funciones y responsabilidades de gestionar su información.

Otra información

Los inventarios de información y otros activos asociados suelen ser necesarios para garantizar protección eficaz de información y se pueden requerir para otros fines, como la salud y seguridad, seguros o razones financieras. Inventarios de información y otros activos asociados también sirven de apoyo a gestión de riesgos, actividades de auditoría, gestión de vulnerabilidad, respuesta a incidentes y planificación de recuperación.

Se pueden delegar tareas y responsabilidades (por ejemplo, a un custodio que cuide activos a diario), 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 conjuntamente para prestar un servicio concreto. En este caso el propietario de este servicio es responsable de la prestación de este incluyendo el funcionamiento de sus activos.

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

5.10 Uso aceptable de información y otros activos asociados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection

Control

Se deberían identificar, documentar y aplicar normas para uso aceptable y procedimientos para el manejo de información y otros activos asociados.

Propósito

Garantizar que información y otros activos asociados se protejan, usen y manejen adecuadamente.

Guía

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

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

a) comportamientos esperados e inaceptables de personas desde de vista de seguridad de información;

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

c) monitoreo de actividades realizadas por la organización.

Se deberían elaborar procedimientos de uso aceptable para todo el ciclo de vida de información en función de su clasificación (ver 5.12) y de riesgos determinados. Se deberían tener en cuenta los siguientes elementos:

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

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

c) protección de las copias temporales o permanentes de información a un nivel coherente con protección de información original;

d) almacenamiento de activos asociados a información de acuerdo con especificaciones de fabricantes (ver 7.8);

e) marcando claramente todas las copias de los soportes de almacenamiento (electrónicos o físicos) a la atención del destinatario autorizado (ver 7.10);

f) autorización de la eliminación de información y otros activos asociados y métodos de eliminación admitidos (ver 8.10).

Otra información

Se puede dar el caso de que los activos en cuestión no pertenezcan directamente a la organización, como servicios de la nube pública. El uso de dichos activos de terceros y cualquier activo de la organización asociado a dichos activos externos (por ejemplo, información, software) se debería identificar según corresponda y controlar, por ejemplo, mediante acuerdos con proveedores de servicios en la nube. También se debería poner especial atención cuando se usa un entorno de trabajo colaborativo.

5.11 Retorno de activos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

Control

Cuando corresponda, el personal y otras partes interesadas deberían devolver todos los bienes de la organización que estén en su poder al cambiar o terminar su empleo contrato o acuerdo.

Propósito

Proteger activos de la organización como parte del proceso de cambio o terminación del empleo contrato o acuerdo.

Guía

El proceso de cambio o terminación se debería formalizar para incluir la devolución de todos activos físicos y electrónicos emitidos anteriormente que sean propiedad de la organización o que se le hayan confiado.

En casos en que personal y otras partes interesadas compren equipo de la organización o usen su propio equipo a personal, se deberían seguir procedimientos para garantizar que toda información relevante se rastrea y se transfiere a la organización y se elimina de forma segura del equipo (ver 7.14).

En casos en que personal y otras partes interesadas tengan conocimientos importantes para las operaciones en curso esa información se debería documentar y transferir a la organización.

Durante el periodo de preaviso y posteriormente, la organización debería impedir copia no autorizada de información relevante (por ejemplo, propiedad intelectual) por parte de personal con preaviso.

La organización debería identificar y documentar claramente toda información y otros activos asociados que se deberían devolver, que puede incluir:

a) dispositivos terminales del usuario;

b) dispositivos de almacenamiento portátiles;

c) equipos especializados;

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 información.

Otra información

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

5.12 Clasificación de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

Control

La Información se debería clasificar de acuerdo con necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y requisitos de partes interesadas.

Propósito

Garantizar la identificación y comprensión de necesidades de protección de información en función de su importancia para la organización.

Guía

La organización debería establecer una política específica sobre clasificación de información y comunicarla a todas partes interesadas.

La organización debería tener en cuenta requisitos de confidencialidad, integridad y disponibilidad en esquema de clasificación.

Las clasificaciones y controles de protección asociados para información deberían tener en cuenta necesidades empresariales para compartir o restringir información, para proteger integridad de información y para garantizar disponibilidad, así como requisitos legales relativos a la confidencialidad, integridad o disponibilidad de información. Activos distintos de información también se pueden clasificar de conformidad con clasificación de información, que se almacena en el activo se procesa con él o se maneja o protege de otro modo.

Los propietarios de información deberían ser responsables de su clasificación.

El esquema de clasificación debería incluir convenciones para clasificación y criterios para revisión de clasificación a lo largo del tiempo. Los resultados de clasificación se deberían actualizar de acuerdo con cambios de valor, sensibilidad y criticidad de información a lo largo de su ciclo de vida.

El esquema debería estar alineado con política específica de control de acceso (ver 5.1) y debería ser capaz de responder a necesidades empresariales específicas de la organización.

La clasificación se puede determinar por el nivel de impacto que el compromiso de información tendría para la organización. Cada nivel definido en esquema debería recibir un nombre que tenga sentido en el contexto de aplicación de esquema de clasificación.

El esquema debería ser coherente en toda la organización e incluir en sus procedimientos para que todos clasifiquen información y demás activos asociados aplicables de la misma manera. Así, todos tienen una comprensión común de requisitos de protección y aplican protección adecuada.

El esquema de clasificación usado dentro de la organización puede ser diferente de los esquemas usados por otras organizaciones, incluso si los nombres de niveles son similares. Además, la información que se mueve entre organizaciones puede variar en su clasificación dependiendo de su contexto en cada organización, incluso si sus esquemas de clasificación son idénticos. Por lo tanto, acuerdos con otras organizaciones que incluyen intercambio de información deberían incluir procedimientos para identificar clasificación de esa información e interpretar niveles de clasificación de otras organizaciones. La relación entre diferentes esquemas se puede determinar buscando la equivalencia en los métodos de tratamiento y protección asociados.

Otra información

La clasificación proporciona a personas que tratan con información una indicación concisa de cómo manejarla protegerla. Creación de grupos de información con necesidades de protección similares y especificación de procedimientos de seguridad de la información que se aplican a toda información de cada grupo facilitan esta tarea. Este enfoque reduce la necesidad de evaluar riesgos caso por caso y de diseñar controles a medida.

La información puede dejar de ser sensible o crítica después de un determinado período de tiempo. Por ejemplo, cuando información se hizo pública ya no tiene requisitos de confidencialidad, pero puede seguir requiriendo protección para sus propiedades de integridad y disponibilidad. Estos aspectos se deberían tener en cuenta ya que una clasificación excesiva puede llevar a aplicación de controles innecesarios que supongan un gasto adicional o por el contrario una clasificación insuficiente puede llevar a que controles sean insuficientes para proteger información de cualquier peligro.

A modo de ejemplo un esquema de clasificación de confidencialidad de información se puede basar en los cuatro niveles siguientes:

a) divulgación no causa ningún daño;

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

c) divulgación tiene un impacto significativo a corto plazo sobre las operaciones u objetivos empresariales;

d) revelación tiene un impacto grave en objetivos empresariales a largo plazo o pone en riesgo la supervivencia de la organización.

5.13 Etiquetado de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_protection	#Defence #Protection

Control

Se debería desarrollar y aplicar un conjunto adecuado de procedimientos para etiquetado de información de acuerdo con esquema de clasificación de información adoptado por la organización.

Propósito

Facilitar la comunicación de clasificación de información y apoyar automatización de tratamiento y gestión de información.

Guía

Los procedimientos de etiquetado de información deberían abarcar información y otros activos asociados en todos los formatos. El etiquetado debería reflejar esquema de clasificación establecido en 5.12. Las etiquetas se deberían reconocer fácilmente. Los procedimientos deberían orientar sobre dónde y cómo se colocan las etiquetas teniendo en cuenta cómo se accede a información o se manejan activos en función de los tipos de soportes de almacenamiento. Los procedimientos pueden definir:

a) casos en que se omite el etiquetado (por ejemplo, el etiquetado de información no confidencial para reducir la carga de trabajo);

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

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

Algunos ejemplos de técnicas de etiquetado son:

a) etiquetas físicas;

b) encabezados y pies de página;

c) metadatos;

d) marca de agua;

e) sellos de goma.

La información digital debería usar metadatos para identificar, gestionar y controlar información, especialmente en que respecta a la confidencialidad. Los metadatos también deberían permitir una búsqueda eficiente y correcta de información. Los metadatos deberían facilitar que sistemas interactúen y tomen decisiones basadas en las etiquetas de clasificación asociadas.

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

Los sistemas deberían añadir metadatos adicionales pertinentes cuando procesen información en función de sus propiedades de seguridad de la información.

El personal y otras partes interesadas deberían conocer procedimientos de etiquetado. Todo personal debería recibir la formación necesaria para garantizar que información se etiquete correctamente y se maneje en consecuencia.

El producto de los sistemas que contienen información clasificada como confidencial o crítica debería llevar una etiqueta de clasificación adecuada.

Otra información

El etiquetado de información clasificada es un requisito fundamental para 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 información y otros activos asociados puede tener a veces efectos negativos. Activos clasificados pueden ser más fáciles de identificar por los actores maliciosos para un posible uso indebido.

Algunos sistemas no etiquetan archivos individuales o registros de base de datos con su clasificación, sino que protegen toda información con el nivel más alto de clasificación de cualquiera de las informaciones que contiene o se permite contener. En estos sistemas es habitual determinar y luego etiquetar información cuando se exporta.

5.14 Transferencia de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

Se deberían establecer normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización, entre la organización y otras partes.

Propósito

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

Guía

Generalidades

La organización debería establecer y comunicar a todas partes interesadas una política específica sobre transferencia de información. Normas, procedimientos y acuerdos para proteger información en tránsito deberían reflejar clasificación de información en cuestión. En que la información se transfiere entre la organización y terceros, se deberían establecer y mantener acuerdos de transferencia (incluyendo autenticación del receptor) para proteger información en todas sus formas en tránsito (ver 5.10).

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

Para todos los tipos de transferencia de información, normas, procedimientos y acuerdos deberían incluir:

a) controles diseñados para proteger información transferida contra interceptación, acceso no autorizado copia, modificación, desvío, destrucción y denegación de servicio incluyendo niveles de control de acceso acordes con clasificación de información en cuestión y cualquier control especial que se requiera para proteger información sensible, como uso de técnicas criptográficas (ver 8.24);

b) controles para garantizar la trazabilidad y no repudio incluyendo mantenimiento de una cadena de custodia de información mientras está en tránsito;

c) identificación de contactos adecuados relacionados con transferencia, incluyendo propietarios de información, propietarios del riesgo los responsables de seguridad y los custodios de información, según proceda;

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

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

f) fiabilidad y disponibilidad del servicio de transferencia;

g) política o directrices específicas de tema sobre uso aceptable de los medios de transferencia de información (ver 5.10);

h) directrices de conservación y eliminación de todos registros empresariales, incluyendo los mensajes;

NOTA Pueden existir legislaciones y normativas locales relativas a la conservación y eliminación de registros empresariales.

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

Transferencia electrónica

Normas, procedimientos y acuerdos también deberían tener en cuenta los siguientes elementos cuando se usan medios de comunicación electrónica para transferencia de información:

a) detención y protección contra los programas maliciosos que se pueden transmitir mediante uso de comunicaciones electrónicas (ver 8.7);

b) protección de información electrónica sensible comunicada en forma de archivo adjunto;

c) prevención del envío de documentos y mensajes en comunicaciones a una dirección o número equivocado;

d) obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales, intercambio de archivos o almacenamiento en la nube;

e) niveles de autenticación más fuertes cuando se transfiere información a través de redes de acceso público;

f) restricciones asociadas a instalaciones de comunicación electrónica (por ejemplo, impedir el reenvío automático del correo electrónico a direcciones de correo externas);

g) proposición a personal y a otras partes interesadas que no envíen mensajes de servicio de mensajes cortos (SMS) o instantáneos con información crítica ya que estos se pueden leer en lugares públicos (y por tanto por personas no autorizadas) o almacenados en dispositivos no protegidos adecuadamente;

h) asesoramiento a personal y a otras partes interesadas sobre problemas de la utilización de las máquinas o servicios de fax, a saber

   1) acceso no autorizado a 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

En que se transfieren medios de almacenamiento físico (incluyendo el papel), normas, procedimientos y acuerdos también deberían incluir:

a) responsabilidades de control y notificación de transmisión, envío y recepción;

b) garantía del correcto direccionamiento y transporte del mensaje;

c) un embalaje que proteja el contenido de cualquier daño físico que se pueda producir durante el transporte y de acuerdo con especificaciones de fabricantes, por ejemplo, protegiéndolo de cualquier factor ambiental que pueda reducir la eficacia de medios de almacenamiento de restauración, como exposición al calor, humedad o campos electromagnéticos; usando normas técnicas mínimas para embalaje y transmisión (por ejemplo, uso de sobres opacos);

d) una lista de empresas de mensajería fiables autorizadas y acordadas por dirección;

e) normas de identificación del mensajero;

f) utilización de controles a prueba de manipulaciones o de manipulación (por ejemplo, bolsas, contenedores), en función del nivel de clasificación de información en medios de almacenamiento que se van a transportar;

g) procedimientos para verificar la identificación de los mensajeros;

h) lista aprobada de terceros que prestan servicios de transporte o mensajería en función de clasificación de información;

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

Transferencia verbal

Para proteger transferencia verbal de información, se debería recordar a personal y a otras partes interesadas que deberían:

a) no mantener conversaciones verbales confidenciales en lugares públicos o a través de canales de comunicación inseguros ya que se pueden escuchar por personas no autorizadas;

b) no dejar mensajes que contengan información confidencial en contestadores automáticos o en mensajes de voz ya que estos se pueden reproducir por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea;

c) filtrar al nivel adecuado para escuchar la conversación;

d) garantizar que se apliquen controles adecuados en la sala (por ejemplo, insonorización, puerta cerrada);

e) iniciar cualquier conversación delicada con un descargo de responsabilidad para que los presentes conozcan el nivel de clasificación y requisitos de manipulación de lo que van a escuchar

Otra información

Sin información.

5.15 Control de acceso

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Las reglas para controlar el acceso físico y lógico a la información y a otros activos asociados se deberían establecer y aplicar en función de los requisitos de seguridad de la empresa y de información.

Propósito

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

Guía

Los propietarios de la información y otros activos asociados deberían determinar requisitos de seguridad de la información y de empresa relacionados con control de acceso. Se debería definir una política específica de control de acceso que tenga en cuenta estos requisitos y que se comunique a todas las partes interesadas pertinentes.

Estos requisitos y política específica del tema deberían tener en cuenta lo siguiente:

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

b) seguridad de las aplicaciones (ver 8.26);

c) acceso físico, que deberían estar respaldado por controles físicos de entrada adecuados (ver 7.2, 7.3 y 7.4);

d) difusión y autorización de información (por ejemplo, principio de necesidad de conocer) y niveles de seguridad de la información y clasificación de esta (ver 5.10, 5.12 y 5.13);

e) restricciones al acceso privilegiado (ver 8.2);

f) separación de funciones (ver 5.3);

g) legislación y reglamentos pertinentes, así como cualquier obligación contractual relativa a la limitación de acceso a datos o servicios (ver 5.31, 5.32, 5.33, 5.34 y 8.3);

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

i) autorización formal de las solicitudes de acceso (ver 5.16 y 5.18);

j) gestión de los derechos de acceso (ver 5.18);

k) registro (ver 8.15).

Las normas de control de acceso se deberían aplicar definiendo, asignando derechos y restricciones de acceso adecuados a entidades pertinentes (ver 5.16). 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 de control de acceso, se pueden asignar funciones específicas a grupos de entidades.

Al momento de definir y aplicar reglas de control de acceso, hay que tener en cuenta lo siguiente:

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

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

c) consideración todos los tipos de conexiones disponibles en entornos distribuidos para que entidades solo tengan acceso a la información y otros activos asociados, incluyendo las redes y servicios de red, que estén autorizados a usar;

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

Otra información

En el contexto del control de acceso se suelen usar principios generales. Dos de los principios más usados son:

a) necesidad de conocer: a una entidad solo se le concede acceso a la información que necesita para realizar sus tareas (diferentes tareas o funciones implican diferentes necesidades de información y, por tanto, diferentes perfiles de acceso);

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

Se debe poner especial atención al especificar las reglas de control de acceso a tener en cuenta:

a) establecimiento de reglas basadas en la premisa del menor privilegio, “Todo está generalmente prohibido a menos que esté expresamente permitido” en lugar de la regla más débil, “Todo está generalmente permitido a menos que esté expresamente prohibido”;

b) cambios en las etiquetas de información (ver 5.13) iniciados automáticamente por las instalaciones de tratamiento de la información y los iniciados a discreción de un usuario;

c) cambios en los permisos de los usuarios iniciados automáticamente por el sistema de información y los iniciados por un administrador;

d) cuándo definir y revisar periódicamente la aprobación.

Las normas de control de acceso deberían estar respaldadas por procedimientos documentados (ver 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) y responsabilidades definidas (ver 5.2, 5.17).

Existen varias formas de implementar control de acceso, como MAC (control de acceso medio), 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 los accesos anteriores o valores específicos del entorno). Las reglas de control de acceso se pueden aplicar con distinta granularidad, desde cobertura de redes o sistemas completos hasta campos de datos específicos y también pueden considerar propiedades como la ubicación de usuario o tipo de conexión de red que se usa para acceso. Estos principios y forma en que se define control de acceso granular pueden tener un impacto significativo en costes. Unas reglas más estrictas y una mayor granularidad suelen suponer un mayor coste. Requisitos de negocio y consideraciones de riesgo se deberían usar para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.

5.16 Gestión de identidad

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Hay que gestionar todo el ciclo de vida de las identidades.

Propósito

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

Guía

Los procesos usados en el contexto de la gestión de la identidad deberían garantizar que:

a) en caso de identidades asignadas a personas, una identidad específica solo se vincula a una única persona para poder responsabilizarla de las acciones realizadas con esta identidad específica;

b) identidades asignadas a varias personas (por ejemplo, las identidades compartidas) solo se permiten en que se necesitan por razones empresariales u operativas, están sujetas a una aprobación y documentación específicas;

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

d) identidades se desactivan o eliminan oportunamente si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o dejan de usar, o si la persona vinculada a una identidad dejó la organización o cambió de función);

e) identidad se asigna a una sola entidad en un dominio específico, [por ejemplo, se evita la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)];

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

La organización debería contar con un proceso de apoyo para manejar los cambios en la información relacionada con las identidades de los usuarios. Estos procesos pueden incluir la nueva verificación de documentos de confianza relacionados con una persona.

En que se usen identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), la organización se debería asegurar de que las identidades de terceros proporcionan el nivel de confianza requerido y de que cualquier riesgo asociado se conoce y se trata suficientemente. Esto puede incluir controles relacionados con los terceros (ver 5.19), así como controles relacionados con la información de autenticación asociada (ver 5.17).

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 empresariales para el establecimiento de una identidad;

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

c) establecer una identidad;

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

e) proporcionar o revocar derechos de acceso específicos a la identidad, sobre base de una autorización adecuada o decisiones sobre derechos (ver 5.18).

5.17 Información de autenticación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Asignación y gestión de la información de autenticación se debería controlar por un proceso de gestión, que incluya asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

Propósito

Para garantizar la correcta autentificación de entidades y evitar fallos en los procesos de autentificación.

Guía

Asignación de información de autenticación

El proceso de asignación y gestión debería garantizar que:

a) contraseñas personales o números de identificación personal (PIN) generados automáticamente durante procesos de inscripción como información secreta temporal de autenticación no sean adivinables, únicas para cada persona y que usuarios estén obligados a cambiarlos después del primer uso;

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

c) información de autenticación, incluida información de autenticación temporal se transmite a usuarios de forma segura (por ejemplo, a través de un canal autenticado y protegido) y se evita el uso de mensajes de correo electrónico no protegidos (texto claro) para este fin;

d) usuarios acusan recibo de información de autenticación;

e) información de autenticación por defecto, predefinida o proporcionada por proveedores, se cambia inmediatamente después de instalación de sistemas o “software”;

f) conservación los registros de los eventos significativos relativos a asignación y gestión de información de autenticación y que se garantice su confidencialidad y que el método de conservación de registros esté aprobado (por ejemplo, mediante uso de una herramienta de bóveda de contraseña aprobada).

Responsabilidades del usuario

Cualquier persona que tenga acceso a la información de autenticación o la use, se debería asegurar de que:

a) la información secreta de autenticación, como contraseñas, se mantiene confidencial. Información secreta de autenticación personal no se debería compartir con nadie. Información secreta de autenticación usada en contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales se comparte únicamente con personas autorizadas;

b) información de autenticación afectada o comprometida se cambia inmediatamente tras notificación o cualquier otro indicio de compromiso;

c) cuando se usen contraseñas como información de autenticación, se seleccionen contraseñas seguras según recomendaciones de las mejores prácticas, por ejemplo:

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

   2) contraseñas no se basan en palabras de diccionario o combinaciones de ellas;

   3) uso de frases de acceso fáciles de recordar y tratar de incluir caracteres alfanuméricos y especiales;

   4) contraseñas tienen una longitud mínima;

d) no uso de mismas contraseñas en distintos servicios y sistemas;

e) obligación de respetar estas normas se incluye también en las condiciones de empleo (ver 6.2).

Sistema de gestión de contraseñas

En que las contraseñas se usan como información de autenticación, el sistema de gestión de contraseñas debería:

a) permitir que usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para solucionar errores de introducción;

b) aplicar contraseñas seguras según recomendaciones de buenas prácticas [ver c) de “Responsabilidades de usuario”];

c) obligar a usuarios a cambiar sus contraseñas en el primer acceso;

d) aplicar cambios de contraseña que sean necesarios, por ejemplo, después de un incidente de seguridad o en caso de cese o cambio de empleo cuando un usuario tenga contraseñas conocidas para identidades que permanezcan activas (por ejemplo, identidades compartidas);

e) evitar reutilización de contraseñas anteriores;

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

g) no mostrar contraseñas en pantalla cuando se introducen;

h) almacenar y transmitir contraseñas de forma protegida.

El cifrado y "hashing" de contraseñas se deberían realizar según técnicas criptográficas aprobadas para contraseñas (ver 8.24).

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 las 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 las normas ISO/IEC 24760.

Exigir cambio frecuente de contraseñas puede ser problemático porque los usuarios se pueden molestar por los cambios frecuentes, olvidar las nuevas contraseñas, anotarlas en lugares poco seguros o elegir contraseñas poco seguras. Provisión de un inicio de sesión único (SSO) u otras herramientas de gestión de autenticación (por ejemplo, bóvedas de contraseñas) reduce cantidad de información de autenticación que usuarios deberían proteger y, por tanto, puede aumentar la eficacia de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de divulgación de información de autenticación.

Algunas aplicaciones requieren que las contraseñas de usuarios sean asignadas por una autoridad independiente. En estos casos, no se aplican apartados a), c) y d) de "Sistema de gestión de contraseñas".

5.18 Derechos de acceso

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Los derechos de acceso a la información y otros activos asociados se deberían proporcionar, revisar, modificar y eliminar de acuerdo con política específica de la organización sobre tema y reglas para control de acceso.

Propósito

Garantizar que acceso a información y a otros activos asociados se defina y autorice de acuerdo con los requisitos de la empresa.

Guía

Provisión y revocación de derechos de acceso

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

a) obtener la autorización del propietario de la información y de otros activos asociados para el uso de la información y de otros activos asociados (ver 5.9). También puede ser conveniente la aprobación por separado de los derechos de acceso por parte de la dirección;

b) considerar requisitos de la empresa, política y normas específicas de la organización en materia de control de acceso;

c) considerar segregación de funciones, incluyendo segregación de roles de aprobación y aplicación de derechos de acceso y separación de roles conflictivos;

d) garantizar eliminación de derechos de acceso cuando alguien no necesite acceder a información y a otros activos asociados, en particular garantizando eliminación oportuna de derechos de acceso de usuarios que hayan abandonado la organización;

e) considerar la posibilidad de conceder derechos de acceso temporales por un período de tiempo limitado y revocarlos en la fecha de expiración, en particular para el personal o acceso temporales requerido por personal;

f) verificar que nivel de acceso concedido se ajusta a políticas específicas de control de acceso (ver 5.15) y es coherente con otros requisitos de seguridad de información, como separación de funciones (ver 5.3);

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

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

i) modificar derechos de acceso de usuarios que cambió de función o de trabajo;

j) eliminar o ajustar derechos de acceso físicos y lógicos, que se puede hacer mediante eliminación, revocación o sustitución de claves, información de autenticación, tarjetas de identificación o suscripciones;

k) mantener un registro de cambios en los derechos de acceso lógicos y físicos de usuarios. Revisión de derechos de acceso.

Revisiones de derechos de acceso

Las revisiones periódicas de los derechos de acceso físico y lógico deberían considerar lo siguiente:

a) derechos de acceso de usuarios después de cualquier cambio dentro de la misma organización (por ejemplo, cambio de trabajo, promoción, descenso) o de terminación de relación laboral (ver 6.1 a 6.5);

b) autorizaciones de derechos de acceso privilegiados.

Consideración antes del cambio o cese de empleo

Los derechos de acceso de un usuario a información y a otros activos asociados se deberían revisar, ajustar o eliminar antes de cualquier cambio o cese de empleo, basándose en evaluación de factores de riesgo como:

a) si el cese o el cambio se inicia por usuario o por la dirección y motivo de cese;

b) las responsabilidades actuales de usuario;

c) el valor de activos actualmente accesibles.

Otra información

Se debería considerar la posibilidad de establecer roles de acceso de usuarios basados en requisitos de empresa que resuman una serie de derechos de acceso en perfiles típicos de acceso de los usuarios. Solicitudes de acceso y revisiones de derechos de acceso son más fáciles de gestionar a nivel de dichos roles que a nivel de derechos particulares.

Se debería considerar la posibilidad de incluir cláusulas en contratos de personal y de servicios que especifiquen las sanciones en caso de que el personal intente acceder sin autorización (ver 5.20, 6.2, 6.4 y 6.6).

En casos de despido iniciado por la dirección, personal descontento o usuarios externos pueden corromper deliberadamente información o sabotear instalaciones de procesamiento de información. En casos de personas que dimiten o son despedidas, pueden tener tentación de recopilar información para su uso futuro.

La clonación es una forma eficiente para que las organizaciones asignen acceso a usuarios. Sin embargo, se debería hacer minuciosamente basándose en distintos roles identificados por la organización en lugar de simplemente clonar una identidad con todos los derechos de acceso asociados. Clonación tiene riesgo inherente de dar lugar a un exceso de derechos de acceso a información y otros activos asociados.

5.19 Seguridad de la información en la relación con los proveedores

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Se deberían definir, aplicar procesos y procedimientos para gestionar riesgos de seguridad de información asociados al uso de productos o servicios de proveedor.

Propósito

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

Guía

La organización debería establecer y comunicar a todas las partes interesadas una política específica sobre relaciones con proveedores.

La organización debería identificar e implementar procesos y procedimientos para abordar riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Esto también se debería aplicar al uso de recursos de proveedores de servicios en la nube por parte de la organización. Estos procesos y procedimientos deberían incluir para que se implementen en la organización, así como los que esta exige al proveedor a aplicar para inicio de utilización de productos o servicios de un proveedor o para terminación de utilización de productos y servicios de un proveedor, como, por ejemplo:

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

b) establecer cómo evaluar y seleccionar a proveedores en función de la sensibilidad de 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 proveedor que tengan controles adecuados de seguridad de información y revisarlos; en particular, exactitud y exhaustividad de controles implementados por proveedor que garantizan integridad de información y procesamiento de información proveedor y, por lo tanto, seguridad de la información de la organización;

d) definir información de la organización, los servicios ICT e infraestructura física a que proveedores pueden acceder, supervisar, controlar o usar;

e) definir tipos de componentes de infraestructura de ICT y servicios prestados por proveedores que pueden afectar a la confidencialidad, integridad y disponibilidad de información de la organización;

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

   1) el uso por parte de los proveedores de información de la organización y otros activos asociados, incluyendo los riesgos originados por el personal potencialmente malintencionado proveedor;

   2) mal funcionamiento o vulnerabilidades de productos (incluyendo los componentes y subcomponentes de “software” usados en estos productos) o servicios prestados por proveedores;

g) supervisar el cumplimiento de los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluyendo revisión por parte de terceros y validación de producto;

h) mitigar el incumplimiento de un proveedor, tanto si se detectó a través de supervisión como por otros medios;

i) manejar incidentes, contingencias asociadas a productos y servicios de los proveedores, incluyendo responsabilidades tanto de la organización como de proveedores;

j) tomar 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) concientizar y formar personal de la organización que interactúa con personal de proveedores en lo que respecta a normas de compromiso adecuadas, políticas, procesos, procedimientos específicos y comportamiento en función de tipo de proveedor y de nivel de acceso de este a sistemas e información de organización;

l) gestionar necesaria transferencia de información, otros activos asociados, cualquier otra cosa que necesite cambiar y garantizar que seguridad de información se mantenga durante todo periodo de transferencia;

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

   1) desaprovisionamiento de derechos de acceso;

   2) manejo de información;

   3) determinación la titularidad de la propiedad intelectual desarrollada durante el compromiso;

   4) portabilidad de información en caso de cambio de proveedor o de “insourcing”;

   5) gestión de registros;

   6) devolución de activos;

   7) eliminación segura de información y otros activos asociados;

   8) requisitos de confidencialidad permanentes;

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

Los procedimientos para continuar con tratamiento de información en caso de que proveedor no pueda suministrar sus productos o servicios (por ejemplo, porque un incidente, porque proveedor ya no está en negocio o ya no proporciona algunos componentes debido a avances tecnológicos) se deberían considerar para evitar cualquier retraso en la organización de productos o servicios de sustitución (por ejemplo, identificación de un proveedor alternativo con antelación o siempre usando proveedores alternativos).

Otra información

En casos en que no es posible que una organización imponga requisitos a un proveedor, la organización debería:

a) considerar las orientaciones dadas en este control a la hora de tomar decisiones sobre elección de un proveedor y su producto o servicio;

b) aplicar los controles compensatorios que sean necesarios sobre base de una evaluación de riesgos.

Los proveedores con una gestión inadecuada de seguridad de la información pueden poner en peligro la información. Se deberían determinar y aplicar controles para gestionar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si existe una necesidad especial de confidencialidad de información, se pueden usar acuerdos de no divulgación o técnicas criptográficas. Otro ejemplo son riesgos de protección de datos personales cuando el acuerdo con el proveedor implica transferencia de información o acceso a ella a través de las fronteras. La organización debería ser consciente que responsabilidad legal o contractual de proteger información sigue siendo de la organización.

También se pueden producir riesgos por controles inadecuados de componentes de infraestructura de ICT o de servicios prestados por proveedores. Mal funcionamiento o vulnerabilidad de componentes o servicios pueden provocar violaciones de seguridad de la información en la organización o en otra entidad (por ejemplo, pueden causar infecciones de “malware[1]”, ataques u otros daños en entidades distintas de la organización).

Ver norma ISO/IEC 27036-2 para más detalles.

5.20 Acercamiento a la seguridad de la información en acuerdos con proveedores

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Requisitos de seguridad de la información pertinentes se deberían establecer y acordar con cada proveedor en función del tipo de relación con él.

Propósito

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

Guía

Se deberían establecer y documentar acuerdos con proveedores para garantizar que existe un claro entendimiento entre la organización y el proveedor respecto a las obligaciones de ambas partes de cumplir con los requisitos pertinentes de seguridad de la información.

1 Del inglés, malware: *programa malicioso, programa maligno, software malicioso o programa informático malintencionado.*

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

a) descripción de información que se va a proporcionar o que se va a acceder y métodos para proveer o entrar a información;

b) clasificación de información según esquema de clasificación de la organización (ver 5.10, 5.12 y 5.13);

c) relación entre esquema de clasificación propio de la organización y esquema de clasificación de proveedor;

d) requisitos legales, estatutarios, reglamentarios y contractuales, incluida protección de datos, tratamiento de información personal identificable (PII), derechos de propiedad intelectual, derechos de autor y una descripción de cómo se garantizará su cumplimiento;

e) obligación de cada parte contractual de aplicar un conjunto de controles acordados, incluyendo control de acceso, revisión de rendimiento, supervisión, elaboración de informes, auditoría y obligaciones de proveedor de cumplir con requisitos de seguridad de información de la organización;

f) normas de uso aceptable de información y otros activos asociados, incluyendo uso inaceptable si es necesario;

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

h) requisitos de seguridad de la información relativos a la infraestructura de ICT de proveedor; en particular, requisitos mínimos de seguridad de información para cada tipo de información y tipo de acceso que sirvan de base para los acuerdos individuales con proveedor, basados en las necesidades empresariales de organización y en criterios de riesgo;

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

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

k) requisitos de formación, concientización para procedimientos específicos y requisitos de seguridad de información (por ejemplo, para la respuesta a incidentes, procedimientos de autorización);

l) disposiciones pertinentes para subcontratación, incluyendo controles que se necesitan aplicar, como acuerdo sobre uso de subproveedores (por ejemplo, exigiendo que estén bajo las mismas obligaciones de proveedor, exigiendo tener una lista de subproveedores y notificación antes de cualquier cambio);

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

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

o) pruebas y mecanismos de garantía de las certificaciones de terceros para requisitos de seguridad de información pertinentes relacionados con procesos de proveedores y un informe independiente sobre eficacia de controles;

p) derecho a auditar los procesos y controles de proveedor relacionados con acuerdo;

q) obligación de proveedor de entregar periódicamente un informe sobre eficacia de controles y acuerdo sobre corrección oportuna de cuestiones pertinentes planteadas en el informe;

r) procesos de resolución de defectos y de conflictos;

s) proporción de una copia de seguridad alineada con necesidades de la organización (en términos de frecuencia y tipo y ubicación de almacenamiento);

t) garantía de disponibilidad de una instalación alternativa (por ejemplo, un sitio de recuperación de catástrofes) que no esté sujeta a mismas amenazas que la instalación principal y consideraciones sobre controles de emergencia (controles alternativos) en caso de que fallen los controles primarios;

u) tenencia de un proceso de gestión de cambios que garantice la notificación previa a la organización y posibilidad de que esta no acepte cambios;

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

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

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

y) disposición de un método de destrucción segura de información de la organización almacenada por proveedor tan pronto como no se requiera;

z) garantías, al final del contrato, traspaso de apoyo a otro proveedor o a la organización de sí mismo.

La organización puede establecer y mantener un registro de acuerdos con partes externas (por ejemplo, contratos, memorandos de entendimiento, acuerdos de intercambio de información) para hacer un monitoreo en que va su información. La organización también debería revisar, validar y actualizar periódicamente sus acuerdos con partes externas para asegurar de que siguen siendo necesarios y se ajustan a su finalidad con cláusulas de seguridad de información pertinentes.

Otra información

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre diferentes tipos de proveedores. Por lo tanto, se debería poner especial atención de incluir todos los requisitos pertinentes para abordar riesgos de seguridad de información.

Para más detalles sobre acuerdos con proveedores, ver norma ISO/IEC 27036. Para acuerdos de servicios en la nube, ver norma ISO/IEC 19086.

5.21 Gestión de seguridad de la información en la cadena de suministro de ICT

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_ security	#Governance_and_ Ecosystem #Protection

Control

Se deberían definir y aplicar procesos y procedimientos para gestionar los riesgos de seguridad de información asociados a cadena de suministro de productos y servicios de ICT.

Propósito

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

Guía

Además de requisitos generales de seguridad de información para relaciones con proveedores, se deberían tener en cuenta los siguientes temas para abordar seguridad de información dentro de seguridad de cadena de suministro de ICT:

a) definir requisitos de seguridad de información para aplicar a adquisición de productos o servicios de ICT;

b) exigir que proveedores de servicios de ICT propaguen requisitos de seguridad de la organización a lo largo de cadena de suministro si subcontratan partes de servicio de ICT prestado a la organización;

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

d) solicitar a proveedores de productos de ICT que proporcionen información que describa componentes de “software” usados en productos;

e) solicitar a proveedores de productos de ICT que proporcionen información que describa funciones de seguridad implementadas de su producto y configuración necesaria para su funcionamiento seguro;

f) aplicar un proceso de supervisión y métodos aceptables para validar que productos y servicios de ICT suministrados cumplen requisitos de seguridad establecidos. Algunos ejemplos de estos métodos de revisión de proveedor pueden ser pruebas de penetración y prueba o validación de certificados de terceros para operaciones de seguridad de información de proveedor;

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

h) obtener garantías que componentes críticos y su origen pueden ser rastreados a lo largo de cadena de suministro;

i) obtener garantías que productos de ICT entregados funcionan como se esperaba, sin ninguna característica inesperada o no deseada;

j) aplicar procesos que garanticen que componentes de proveedores son auténticos y no se alteró con respecto a su especificación. Algunos ejemplos de medidas son etiquetas antimanipulación, verificaciones “hash” criptográficas o firmas digitales. Control de prestaciones fuera de especificación puede ser un indicador de manipulación o falsificación. Prevención y detección de manipulaciones se deberían aplicar en múltiples etapas de ciclo de vida de desarrollo de sistema, incluyendo diseño, desarrollo, integración, operaciones y mantenimiento;

k) obtener garantías de que productos de ICT alcanzan niveles de seguridad requeridos, por ejemplo, mediante una certificación formal o un esquema de evaluación como el Acuerdo de Reconocimiento de Criterios Comunes;

l) definir reglas para compartir información relativa a cadena de suministro, cualquier problema y compromiso potencial entre la organización y proveedores;

m) aplicar procesos específicos para gestionar el ciclo de vida y disponibilidad de componentes de ICT y riesgos de seguridad asociados. Esto incluye gestión de riesgos que componentes dejen de estar disponibles debido a que proveedores ya no están en el negocio o a que proveedores ya no proporcionan estos componentes debido a avances tecnológicos. Se debería considerar la identificación de un proveedor alternativo, proceso de transferencia de “software” y competencias al proveedor alternativo.

Otra información

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

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

El ICT se debería adquirir de fuentes acreditadas. La fiabilidad de “software” y de “hardware” es una cuestión de control de calidad. Aunque generalmente no es posible que una organización inspeccione sistemas de control de calidad de sus proveedores, puede hacer juicios fiables basados en la reputación del proveedor.

Cadena de suministro de ICT, tal como se aborda aquí, incluye los servicios en la nube.

Ejemplos de cadenas de suministro de ICT son:

a) suministro de servicios en la nube, en que el proveedor de servicios en la nube se apoya en los desarrolladores de “software”, proveedores de servicios de telecomunicaciones y de “hardware”;

b) “IoT”, en que el servicio implica a fabricantes de dispositivos, a proveedores de servicios en la nube (por ejemplo, los operadores de plataformas “IoT”), a desarrolladores de aplicaciones móviles y Web, proveedor de bibliotecas de “software”;

c) servicios de alojamiento, en que el proveedor se apoya en mesas de servicio externas, incluyendo primeras, segundas y tercer nivel de apoyo.

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

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

5.22 Monitoreo, revisión y gestión de cambios de servicios del proveedor

Tipo de control	Propiedades de la seguridad de información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_ security #Information_ security_ assurance	#Governance_and_ Ecosystem #Protection #Defence

Control

La organización debería supervisar, revisar, evaluar y gestionar regularmente los cambios en prácticas de seguridad de información de proveedores y la prestación de servicios.

Propósito

Mantener un nivel acordado de seguridad de información y de prestación de servicios conforme a acuerdos con proveedores.

Guía

Monitoreo, revisión y gestión de cambios de servicios de proveedores deberían garantizar el cumplimiento de condiciones de seguridad de información de acuerdos, gestión adecuada de incidentes y problemas de seguridad de información y que cambios en servicios de proveedores o en situación de empresa no afecten a prestación de servicio.

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

a) controlar niveles de rendimiento de servicio para verificar cumplimiento de acuerdos;

b) controlar cambios realizados por proveedores, entre otros:

   1) mejorar servicios actuales ofrecidos;

   2) desarrollar nuevas aplicaciones y sistemas;

   3) modificar o actualizar políticas y procedimientos de proveedor;

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

c) supervisar cambios en servicios de proveedores, incluyendo:

   1) cambiar y mejorar redes;

   2) usar nuevas tecnologías;

   3) adoptar nuevos productos o nuevas versiones o lanzamientos;

   4) utilizar nuevas herramientas y entornos de desarrollo;

   5) cambiar la ubicación física de instalaciones de servicio;

   6) cambiar de subproveedores;

   7) Subcontratar a otro proveedor;

d) revisar informes de servicio elaborados por proveedor y organizar reuniones periódicas sobre progresos realizados, tal y como exigen acuerdos;

e) realizar auditorías de proveedores y subproveedores, junto con revisión de informes de auditores independientes, si están disponibles y hacer un seguimiento de problemas identificados;

f) proporcionar información sobre incidentes de seguridad de la información y revisar esta información según exigido por acuerdos y cualquier directriz y procedimiento de apoyo;

g) revisar pistas de auditoría de proveedores y registros de eventos de seguridad de información, problemas operativos, fallos, el monitoreo de averías e interrupciones relacionadas con 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 aspectos de seguridad de la información de relaciones de proveedor con sus propios proveedores;

k) garantizar que el proveedor mantiene una capacidad de servicio suficiente, junto con planes viables diseñados para garantizar que niveles de continuidad de servicio acordados se mantienen tras fallos importantes de servicio o catástrofes (ver 5.29, 5.30, 5.35, 5.36, 8.14);

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

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

La responsabilidad de gestión de relaciones con proveedores se debería asignar a una persona o designar un equipo. Se deberían poner a disposición de proveedores los conocimientos técnicos y recursos suficientes para supervisar cumplimiento de requisitos de acuerdo, en particular los relativos a seguridad de la información. Se deberían tomar medidas adecuadas cuando se observen deficiencias en la prestación de servicio.

Otra información

Ver norma ISO/IEC 27036-3 para más detalles.

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relationships_ security	#Gobierno_y_Ecosistema #Protección

Control

Procesos de adquisición, uso, gestión y salida de servicios en la nube se deberían establecer de acuerdo con requisitos de seguridad de la información de la organización.

Propósito

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

Guía

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

La organización debería definir y comunicar cómo pretende gestionar riesgos de seguridad de la información asociados uso de servicios en la nube. Puede ser una extensión o parte del enfoque existente sobre cómo una organización gestiona servicios proporcionados por partes externas (ver 5.21 y 5.22).

Uso de servicios en la nube puede implicar una responsabilidad compartida en materia de seguridad de la información y un esfuerzo de colaboración entre proveedor de servicios en la nube y la organización que actúa como cliente de dichos servicios. Es esencial que responsabilidades tanto de proveedor de servicios en la nube como de la organización, que actúa como cliente de servicios en la nube, se definan y apliquen adecuadamente.

La organización debería definir:

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

b) criterios de selección de servicios en la nube y ámbito de utilización de servicios en la nube;

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

d) qué controles de seguridad de la información son gestionados por proveedor de servicios en la nube y cuáles son gestionados por la organización como cliente de servicios en la nube;

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

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

g) cómo gestionar controles, las interfaces y los cambios en servicios cuando una organización usa varios servicios en la nube, especialmente de diferentes proveedores de servicios en la nube;

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

i) enfoque para supervisar, revisar y evaluar uso continuo de servicios en la nube para gestionar riesgos de seguridad de la información;

j) cómo cambiar o dejar de usar servicios en la nube, incluyendo estrategias de salida de servicios en la nube.

Los acuerdos de servicios en la nube suelen estar predefinidos y no están abiertos a la negociación. Para todos servicios en la nube, la organización debería revisar acuerdos de servicios en la nube con proveedor o proveedores de servicios en la nube. Un acuerdo de servicio en la nube debería abordar requisitos de confidencialidad, integridad, disponibilidad y manejo de información de la organización, con objetivos adecuados de nivel de servicio en la nube y objetivos cualitativos de servicio en la nube. La organización también debería realizar las evaluaciones de riesgo pertinentes para identificar riesgos asociados uso de servicio en la nube. Cualquier riesgo residual relacionado con uso de servicio en la nube se debería identificar y aceptar claramente por la dirección apropiada de la organización.

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

a) proporcionar soluciones basadas en normas de arquitectura e infraestructura aceptadas por el sector;

b) gestionar controles de acceso de servicio en la nube para satisfacer requisitos de la organización;

c) aplicar soluciones de vigilancia y protección contra el malware;

d) procesar y almacenar la información sensible de la organización en lugares aprobados (por ejemplo, un país o región concretos) o dentro de una jurisdicción determinada o sujeta a ella;

e) proporcionar apoyo dedicado en caso de un incidente de seguridad de información en entorno de servicios en la nube;

f) garantizar cumplimiento de requisitos de seguridad de la información de la organización en caso de que servicios en la nube se subcontraten de nuevo a un proveedor externo (o prohibir que se subcontraten servicios en la nube);

g) apoyar a la organización en la recopilación de pruebas digitales, teniendo en cuenta leyes y reglamentos sobre pruebas digitales en distintas jurisdicciones;

h) proporcionar un soporte adecuado y disponibilidad de servicios durante un periodo de tiempo apropiado cuando la organización quiera salir de servicio en la nube;

i) proporcionar las copias de seguridad necesarias de datos y la información de configuración y gestionar de forma segura las copias de seguridad, según proceda, en función de las capacidades de proveedor de servicios en la nube usado por la organización, que actúa como cliente de servicios 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 de servicio en la nube, cuando se solicite durante la prestación de servicio o al finalizarlo.

La organización, actuando como cliente de servicios en la nube, debería considerar si el acuerdo debería exigir a proveedores de servicios en la nube que proporcionen una notificación previa antes de realizar cualquier cambio sustancial que afecte al cliente en la forma en que se presta servicio a la organización, incluyendo:

a) cambios en infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios de "hardware" o "software") que afecten o cambien la oferta de servicios en la nube;

b) procesos o almacenamiento de información en una nueva jurisdicción geográfica o legal;

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

La organización que usa servicios en la nube debería mantener un estrecho contacto con sus proveedores de servicios en la nube. Estos contactos permiten intercambio mutuo de información sobre seguridad de la información para uso de servicios en la nube, incluyendo un mecanismo para que tanto proveedor de servicios en la nube como la organización, actuando como cliente de servicios en la nube, puedan supervisar cada característica de servicio e informar de incumplimientos de compromisos contenidos en acuerdos.

Otra información

Este control considera seguridad en la nube desde la perspectiva de cliente de servicios de esta.

Se puede encontrar información adicional relacionada con servicios en la nube en ISO/IEC 17788, ISO/IEC 17789 e ISO/IEC 22123-1. Detalles relacionados con portabilidad de la nube en apoyo de estrategias de salida se pueden encontrar en norma ISO/IEC 19941. Aspectos específicos relacionados con seguridad de información y servicios en la nube pública se describen en norma ISO/IEC 27017. Detalles relacionados con protección de la información personal en las nubes públicas que actúan como procesador de información personal se describen en norma ISO/IEC 27018. Relaciones con proveedores de servicios en la nube están cubiertas por norma ISO/IEC 27036-4 y acuerdos de servicios en la nube y su contenido se tratan en serie ISO/IEC 19086, con la seguridad y privacidad específicamente cubiertas por norma ISO/IEC 19086-4.

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

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

Control

La organización debería planificar y preparar para gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos de gestión de incidentes de seguridad de la información, funciones y responsabilidades.

Propósito

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

Guía

Funciones y responsabilidades

La organización debería establecer procesos adecuados de gestión de incidentes de seguridad de la información. Se deberían determinar funciones y responsabilidades para llevar a cabo procedimientos de gestión de incidentes y comunicarlas eficazmente a las partes interesadas internas y externas pertinentes.

Hay que tener en cuenta lo siguiente:

a) establecer un método común para notificar los sucesos relacionados con seguridad de la información, incluyendo punto de contacto (ver 6.8);

b) establecer un proceso de gestión de incidentes que proporcione a la organización capacidad de gestionar incidentes de seguridad de la información, incluyendo la administración, documentación, detección, triaje, priorización, análisis, comunicación y coordinación de las partes interesadas;

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

d) permitir que solo el personal competente se ocupe de las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización. Dicho personal debería recibir documentación sobre procedimientos y formación periódica;

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

Procedimientos de gestión de incidentes

Los objetivos de gestión de incidentes de seguridad de la información se deberían acordar con la dirección y debería garantizar que los responsables de gestión de incidentes de seguridad de la información comprendan las prioridades de la organización para gestionar incidentes de seguridad de la información, incluyendo plazo de resolución basado en las posibles consecuencias y gravedad. Procedimientos de gestión de incidentes se deberían implementar para cumplir con estos objetivos y prioridades.

La dirección debería asegurar que se elaborara un plan de gestión de incidentes de seguridad de la información que contemple diferentes escenarios y se desarrollen e implementen procedimientos para las siguientes actividades:

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

b) supervisión (ver 8.15 y 8.16), supervisión (ver 8.16), clasificación (ver 5.25), análisis y la notificación (ver 6.8) de eventos e incidentes de seguridad de la información (por medios humanos o automáticos);

c) gestión de incidentes de seguridad de la información hasta su conclusión, incluyendo respuesta y escalada (ver 5.26), según el tipo y categoría de incidente, la posible activación de gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación a las partes interesadas internas y externas;

d) coordinación con las partes interesadas internas y externas, como autoridades, grupos y foros de interés externos, proveedores y clientes (ver 5.5 y 5.6);

e) registro de actividades de gestión de incidentes;

f) manejo de pruebas (ver 5.28);

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

h) identificación de lecciones aprendidas y de mejoras necesarias en procedimientos de gestión de incidentes o en controles de seguridad de la información en general.

Procedimientos de notificación

Procedimientos de información deberían incluir:

a) medidas que se deberían tomar en caso de que se produzca un evento de seguridad de la información (por ejemplo, anotar inmediatamente todos los detalles pertinentes, como el mal funcionamiento que se produzca y mensajes que aparezcan en pantalla, informar inmediatamente al punto de contacto y tomar únicamente medidas coordinadas);

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

c) procesos adecuados de retroalimentación para garantizar que personas que informan de sucesos relacionados con seguridad de la información se notifiquen, en la medida de lo posible, de resultados después que se abordó y cerró el problema;

d) creación de informes de incidentes.

Cualquier requisito externo sobre notificación de incidentes a las partes interesadas pertinentes dentro de plazo definido (por ejemplo, requisitos de notificación de infracciones a los reguladores) se debería tener en cuenta a la hora de aplicar procedimientos de gestión de incidentes.

Otra información

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

En la norma ISO/IEC 27035 se ofrecen orientaciones detalladas sobre gestión de incidentes de seguridad de la información.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective	#Confidentiality #Integrity #Availability	#Detectar #Respond	#Information_security_event_management	#Defence

Control

La organización debería evaluar eventos de seguridad de la información y decidir si deberían categorizar como incidentes de seguridad de información.

Propósito

Garantizar la categorización y priorización efectiva de eventos de seguridad de la información.

Guía

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

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

Los resultados de evaluación y la decisión se deberían registrar detalladamente a efectos de referencia y verificación futuras.

Otra información

La norma ISO/IEC 27035 proporciona guía sobre gestión de incidentes.

5.26 Respuesta a incidentes de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Control

Los incidentes de seguridad de la información se deberían responder de acuerdo con procedimientos documentados.

Propósito

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

Guía

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

Un equipo designado con la competencia requerida debería responder por los incidentes de seguridad de la información (ver 5.24).

La respuesta debería incluir lo siguiente:

a) contener, si consecuencias de incidente se pueden extender, sistemas afectados por el mismo;

b) recoger pruebas (ver 5.28) lo antes posible después del suceso;

c) escalar, según sea necesario, incluyendo actividades de gestión de crisis y posiblemente invocando planes de continuidad de negocio (ver 5.29 y 5.30);

d) garantizar que todas actividades de respuesta implicadas se registren adecuadamente para su posterior análisis;

e) comunicar la existencia de 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 conocimiento;

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

g) una vez que el incidente se resuelva con éxito, cerrarlo formalmente y registrarlo;

h) realizar análisis forenses de seguridad de la información, según sea necesario (ver 5.28);

i) realizar un análisis posterior al incidente para identificar la causa raíz. Garantizar que se documenta y se comunica de acuerdo con procedimientos definidos (ver 5.27);

j) identificar y gestionar las vulnerabilidades y debilidades de seguridad de la información, incluyendo las relacionadas con controles que han causado, contribuido o no han evitado el incidente.

Otra información

La norma ISO/IEC 27035 proporciona guía sobre gestión de incidentes.

5.27 Aprendizaje sobre incidentes de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence

Control

Se deberían usar conocimientos obtenidos de incidentes de seguridad de la información para reforzar y mejorar controles de seguridad de la información.

Propósito

Reducir la probabilidad o consecuencias de futuros incidentes.

Guía

La organización debería establecer procedimientos para cuantificar y controlar los tipos, volúmenes y costes de incidentes de seguridad de la información.

La información obtenida de evaluación de incidentes de seguridad de la información se debería usar para:

a) mejorar el plan de gestión de incidentes, incluyendo los escenarios y procedimientos de incidentes (ver 5.24);

b) identificar incidentes recurrentes o graves y sus causas para actualizar evaluación de riesgos de seguridad de información de la organización, determinar y aplicar controles adicionales necesarios para reducir la probabilidad o consecuencias de futuros incidentes similares. Mecanismos que permiten esto incluyen la recopilación, cuantificación y monitoreo de información sobre los tipos, volúmenes y costes de incidentes;

c) mejorar concientización y formación de usuarios (ver 6.3) proporcionando ejemplos de lo que puede ocurrir, cómo responder a esos incidentes y cómo evitarlos en el futuro.

Otros datos

La norma ISO/IEC 27035 proporciona guía.

5.28 Recolección de pruebas

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Corrective	#Confidentiality #Integrity #Availability	#Detectar #Respond	#Information_security_event_management	#Defence

Control

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

Propósito

Garantizar una gestión coherente y eficaz de pruebas relacionadas con incidentes de seguridad de la información a efectos de acciones disciplinarias y legales.

Guía

Se deberían desarrollar y seguir procedimientos internos a la hora de tratar pruebas relacionadas con eventos de seguridad de la información a efectos de acciones disciplinarias y legales. Se deberían tener en cuenta requisitos de distintas jurisdicciones para maximizar las posibilidades de admisión en las jurisdicciones pertinentes.

En general, estos procedimientos para gestión de pruebas deberían proporcionar instrucciones para identificación, recogida, adquisición y conservación de pruebas de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y estado de dispositivos (por ejemplo, encendidos o apagados). Por lo general, pruebas se deberían recoger de manera que se admitan en tribunales nacionales correspondientes o en otro foro disciplinario. Se debería poder demostrar:

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

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

c) cualquier sistema de información que se hayan obtenido pruebas funcionaba correctamente en el momento en que se registraron pruebas.

Se debería buscar una certificación (cuando esté disponible) u otros medios pertinentes de cualificación de personal y de herramientas, a fin de reforzar el valor de pruebas conservadas.

Las pruebas digitales pueden trascender los límites organizativos o jurisdiccionales. En tales casos, se debería garantizar que la organización está facultada para recoger información requerida como prueba digital.

Otra información

Cuando se detecta por primera vez un suceso relacionado con seguridad de la información, no siempre es evidente si el suceso dará lugar a una acción judicial o no. Por lo tanto, existe el peligro que las pruebas necesarias se destruyan intencionada o accidentalmente antes que se perciba gravedad de incidente. Es aconsejable involucrar a la asesoría legal o a fuerzas orden en una etapa temprana de cualquier acción legal contemplada y asesorar sobre pruebas necesarias.

La norma ISO/IEC 27037 proporciona definiciones y directrices para identificación, recogida, adquisición y conservación de pruebas digitales.

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

5.29 Seguridad de la información durante interrupción

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

Control

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

Propósito

Proteger información y otros activos asociados durante interrupción.

Guía

La organización debería determinar sus requisitos para adaptar controles de seguridad de la información durante interrupción. Los requisitos de seguridad de la información se deberían incluir en procesos de gestión de continuidad del negocio.

Se deberían desarrollar, implementar, probar, revisar y evaluar planes para mantener o restaurar seguridad de información de procesos críticos de negocio tras una interrupción o fallo. La seguridad de la información se debería restaurar al nivel y en los plazos requeridos.

La organización debería implementar y mantener:

a) controles de seguridad de información, sistemas y herramientas de apoyo en el marco de planes de continuidad de actividades y de ICT;

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

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

Otra información

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

Información sobre sistemas de gestión de continuidad del negocio se puede encontrar en las normas ISO 22301 e ISO 22313. En la norma ISO/TS 22317 se ofrecen más orientaciones sobre análisis del impacto en el negocio (BIA).

5.30 Preparación de ICT para continuidad de actividad

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Corrective	#Availability	#Respond	#Continuity	#Resilience

Control

La preparación de ICT se debería planificar, aplicar, mantener y probar en función de objetivos de continuidad de actividad y de requisitos de continuidad de ICT.

Propósito

Garantizar disponibilidad de la información de la organización y otros activos asociados durante las interrupciones.

Guía

La preparación de ICT para continuidad de actividad es un componente importante en gestión de continuidad de actividad y gestión de seguridad de la información para garantizar que objetivos de la organización puedan seguir cumpliéndose durante interrupción.

Los requisitos de continuidad de ICT son el resultado de análisis de impacto en el negocio (BIA). El proceso de BIA debería usar tipos de impacto y criterios para evaluar los impactos a lo largo del tiempo resultantes de interrupción de actividades empresariales que ofrecen productos y servicios. La magnitud y duración del impacto resultante se deberían usar para identificar actividades prioritarias a las que se debería asignar un objetivo de tiempo de recuperación (RTO). El BIA debería entonces determinar qué recursos son necesarios para apoyar actividades prioritarias. También se debería especificar un RTO para estos recursos. Un subconjunto de estos recursos debería incluir servicios de ICT.

El BIA que implica a servicios de ICT se puede ampliar para definir requisitos de rendimiento y capacidad de sistemas de ICT y objetivos de punto de recuperación (RPO) de la información necesarios para apoyar actividades durante interrupción.

Sobre la base de resultados del BIA y de evaluación de riesgos que afectan a servicios de ICT, la organización debería identificar y seleccionar estrategias de continuidad de ICT que consideren opciones para antes, durante y después de interrupción. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. Sobre la base de estrategias, se deberían desarrollar, implementar y probar planes para cumplir con el nivel de disponibilidad requerido de servicios de ICT y en los plazos requeridos tras interrupción o el fallo de procesos críticos.

La organización debería garantizar:

a) existencia de una estructura organizativa adecuada para preparar, mitigar y responder a una perturbación con el apoyo de personal con la responsabilidad, autoridad y competencia necesarias;

b) planes de continuidad de ICT, incluyendo procedimientos de respuesta y recuperación que detallan cómo la organización está planeando gestionar una interrupción de servicio de ICT:

   1) evaluación regular mediante ejercicios y pruebas;

   2) aprobación por la dirección;

c) planes de continuidad de ICT incluyen la siguiente información de continuidad de ICT:

   1) especificaciones de rendimiento y capacidad para cumplir requisitos y objetivos de continuidad de actividad, tal como se especifica en el BIA;

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

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

Otra información

La gestión de continuidad de ICT constituye una parte fundamental de requisitos de continuidad de actividad en lo que respecta a disponibilidad para poder:

a) responder y recuperar la interrupción de servicios de ICT, independientemente de la causa;

b) garantizar continuidad de actividades prioritarias con el apoyo de servicios ICT necesarios;

c) responder antes que se produzca una interrupción de servicios de ICT y tras supervisión de al menos un incidente que pueda dar lugar a una interrupción de servicios de ICT.

En la norma ISO/IEC 27031 se ofrecen más orientaciones sobre la preparación de ICT para la continuidad de las actividades.

En las normas ISO 22301 e ISO 22313 se ofrecen más orientaciones sobre sistemas de gestión de la continuidad del negocio.

En la norma ISO/TS 22317 se ofrece guía sobre el BIA.

5.31 Requisitos legales, reglamentarios y contractuales

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_ Ecosystem #Protection

Control

Requisitos legales, estatutarios, reglamentarios y contractuales relevantes para seguridad de la información y enfoque de la organización para cumplir con estos requisitos se deberían identificar, documentar y mantener al día.

Propósito

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

Guía

Generalidades

Requisitos externos, incluyendo los legales, reglamentarios o contractuales, se deberían tener en cuenta al momento de:

a) desarrollar políticas y procedimientos de seguridad de información;

b) diseñar, aplicar o modificar los controles de seguridad de información;

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

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

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

f) determinar requisitos contractuales de proveedores pertinentes para la organización y alcance de suministro de productos y servicios.

Legislación y normativa

La organización debería:

a) identificar toda la legislación y normativa relevante para seguridad de información de la organización con fin de conocer requisitos para su tipo de negocio;

b) tener en cuenta el cumplimiento en todos los países pertinentes, si la organización:

   — realizar negocios en otros países;

   — usar productos y servicios de otros países en que la legislación y normativa pueden afectar a la organización;

   — transferir información a través de las fronteras jurisdiccionales en que las leyes y reglamentos pueden afectar a la organización;

c) revisar periódicamente legislación y normativa identificadas para estar al día de cambios e identificar la nueva legislación;

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

Criptografía

La criptografía es un área que suele tener requisitos legales específicos. Se debería tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos pertinentes relativos a los siguientes puntos:

a) restricciones a la importación o exportación de equipos y programas informáticos para realizar funciones criptográficas;

b) restricciones a la importación o exportación de equipos y programas informáticos diseñados para incorporar funciones criptográficas;

c) restricciones en el uso de la criptografía;

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

e) validez de las firmas digitales, sellos y certificados.

Se recomienda buscar asesoramiento jurídico para garantizar el cumplimiento de legislación y normativa pertinentes, especialmente cuando la información cifrada o herramientas de criptografía se mueven a través de fronteras jurisdiccionales.

Contratos

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

a) contratos con clientes;

b) contratos con proveedores (ver 5.20);

c) contratos de seguros.

Otra información

Sin información.

5.32 Derechos de propiedad intelectual

Tipo de control	Información propiedades de seguridad	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_ Ecosystem

Control

La organización debería aplicar procedimientos adecuados para proteger los derechos de propiedad intelectual.

Propósito

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

Guía

Se deberían tener en cuenta las siguientes directrices para proteger cualquier material que se pueda considerar propiedad intelectual:

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

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

c) adquirir programas informáticos solo a través de fuentes conocidas y acreditadas, para garantizar que no se infringen derechos de autor;

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

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

f) garantizar que no se supere el número máximo de usuarios o recursos [por ejemplo, unidades centrales de procesamiento (CPU)] permitidos en la licencia;

g) realizar revisiones para garantizar que solo se instalan los programas informáticos y productos con licencia autorizados;

h) proporcionar procedimientos para mantener condiciones adecuadas de licencia;

i) proporcionar procedimientos para eliminar o transferir el “software” a otros;

j) cumplimiento de condiciones de programas informáticos y de información obtenida de redes públicas y fuentes externas;

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

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

Otra información

Derechos de propiedad intelectual incluyen derechos de autor de programas o documentos, derechos de diseño, marcas, las patentes y licencias de código fuente.

Lo propietarios suelen suministrar los productos de “software” bajo un acuerdo de licencia que especifica términos y condiciones de esta, por ejemplo, limitando el uso de productos a máquinas específicas o limitando la copia a creación de estas de seguridad únicamente. Ver norma ISO/IEC 19770 para más detalles sobre gestión de activos de IT.

Los datos se pueden adquirir en fuentes externas. Por lo general, estos datos se obtienen bajo los términos de un acuerdo de intercambio de datos o un instrumento legal similar. Estos acuerdos de intercambio de datos deberían dejar claro qué tratamiento se permite para los datos adquiridos. También es aconsejable que se indique claramente la procedencia de los datos. Ver norma ISO/IEC 23751 para más detalles sobre los acuerdos de intercambio de datos.

Los requisitos legales, estatutarios, reglamentarios y contractuales pueden imponer restricciones a la copia de material de propiedad. En particular, pueden exigir que solo se pueda usar material desarrollado por la organización o que el desarrollador autorizó o proporcionó a la organización. Cualquier infracción de los derechos de autor puede dar lugar a acciones legales, que pueden implicar multas y procedimientos penales.

Además de la necesidad de la organización de cumplir con sus obligaciones respecto a derechos de propiedad intelectual de terceros, también se deberían gestionar los riesgos de que el personal y los terceros no respeten los propios derechos de propiedad intelectual de la organización.

5.33 Protección de registros

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Protection

Control

Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.

Propósito

Garantizar cumplimiento de requisitos legales, reglamentarios y contractuales, así como expectativas de comunidad o de sociedad relacionadas con protección y disponibilidad de registros.

Guía

La organización debería tomar las siguientes medidas para proteger la autenticidad, la fiabilidad, la integridad y la usabilidad de los documentos de archivo ya que su contexto empresarial y los requisitos para su gestión cambian con el tiempo:

a) emitir directrices sobre almacenamiento, manejo de la cadena de custodia y eliminación de registros, que incluya prevención de manipulación de estos. Estas directrices deberían estar en consonancia con la política específica de la organización en materia de gestión de registros y otros requisitos de estos;

b) elaborar un calendario de conservación en que se definan registros y periodo de tiempo durante que se deberían conservar.

El sistema de almacenamiento y manipulación debería garantizar identificación de registros y su período de conservación teniendo en cuenta la legislación o normativa nacional o regional, así como expectativas de comunidad o sociedad, si procede. Este sistema debería permitir la destrucción adecuada de registros después de ese período si la organización no los necesita.

Al momento de decidir sobre protección de registros específicos de la organización, se debería considerar su correspondiente clasificación de seguridad de la información, basada en esquema de clasificación de la organización. Los registros se deberían clasificar en tipos de registros (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles de períodos de retención y tipo de medios de almacenamiento permitidos que pueden ser físicos o electrónicos.

Los sistemas de almacenamiento de datos se deberían elegir de manera que los registros requeridos se puedan recuperar en un plazo y formato aceptables, en función de los requisitos que se deban cumplir.

Al elegir un medio de almacenamiento electrónico, se deberían establecer procedimientos que garanticen la capacidad de acceso a documentos de archivo (tanto a los medios de almacenamiento como a la legibilidad del formato) durante todo el período de conservación, para evitar pérdidas debidas a futuros cambios tecnológicos. Claves criptográficas y programas asociados a archivos encriptados o a las firmas digitales también se deberían conservar para permitir el descifrado de registros durante el período de conservación de estos (ver 8.24).

Los procedimientos de almacenamiento y manipulación se deberían aplicar de acuerdo con las recomendaciones proporcionadas por los fabricantes de medios de almacenamiento. Se debería tener en cuenta la posibilidad de deterioro de los soportes usados para el almacenamiento de los registros.

Otra información

Los registros documentan eventos o transacciones individuales o pueden formar agregaciones que se diseñó para documentar procesos de trabajo, actividades o funciones. Son a la vez pruebas de actividad empresarial y activos de información. Cualquier conjunto de información, independientemente de su estructura o forma, se puede gestionar como un registro. Esto incluye información en forma de documento, una colección de datos u otros tipos de información digital o analógica que se crean, capturan y gestionan en el curso de actividad empresarial.

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

Puede ser necesario conservar algunos registros de forma segura para cumplir con los requisitos legales, reglamentarios o contractuales, así como para apoyar actividades empresariales esenciales. Las leyes o reglamentos nacionales pueden establecer el período de tiempo y contenido de datos para conservación de información. Para mayor información sobre gestión de registros, ver la norma ISO 15489.

5.34 Privacidad y protección de PII

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection

Control

La organización debería identificar y cumplir requisitos relativos a preservación de la privacidad y protección de PII de acuerdo con leyes, reglamentos aplicables y requisitos contractuales.

Propósito

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

Guía

La organización debería establecer, comunicar una política específica sobre privacidad y protección de PII a todas las partes interesadas pertinentes.

La organización debería desarrollar e implementar procedimientos para la preservación de privacidad y protección de PII. Dichos procedimientos se deberían comunicar a todas partes interesadas que participen en el tratamiento de información personal identificable.

El cumplimiento de estos procedimientos y de toda la legislación y reglamentos pertinentes relativos a la preservación de privacidad y protección de la información personal requiere funciones, responsabilidades y controles adecuados. A menudo, la mejor manera de lograrlo es designando a una persona responsable, como un funcionario de privacidad, que debería orientar al personal, a proveedores de servicios y a otras partes interesadas sobre sus responsabilidades individuales y procedimientos específicos que se deberían seguir.

La responsabilidad de tratamiento de información de identificación personal se debería abordar teniendo en cuenta la legislación y reglamentos pertinentes.

Se deberían aplicar medidas técnicas y organizativas adecuadas para proteger la información personal.

Otra información

Varios países introdujeron una legislación que establece controles sobre recogida, tratamiento, transmisión y supresión de información de identificación personal. Dependiendo de legislación nacional respectiva, dichos controles pueden imponer obligaciones a quienes recogen, procesan y difunden PII y también pueden restringir la autoridad para transferir PII a otros países.

La norma ISO/IEC 29100 proporciona un marco de alto nivel para protección de PII en sistemas de ICT. En la norma ISO/IEC 27701 se puede encontrar más información sobre sistemas de gestión de la información sobre privacidad. Información específica sobre gestión de información sobre la privacidad para las nubes públicas que actúan como procesadores de PII se puede encontrar en la norma ISO/IEC 27018.

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

5.35 Revisión independiente de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem

Control

El enfoque de la organización para gestión de seguridad de información y su aplicación, incluyendo personas, procesos y tecnologías, se debería revisar de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Propósito

Garantizar la idoneidad, adecuación y eficacia continuas de enfoque de organización para gestionar seguridad de información.

Guía

La organización debería contar con procesos para realizar revisiones independientes.

La dirección debería planificar e iniciar revisiones periódicas independientes. Las revisiones deberían incluir evaluación de oportunidades de mejora y necesidad de cambios en enfoque de seguridad de información, incluida política de seguridad de información, políticas de temas específicos y otros controles.

Dichas revisiones se deberían llevar a cabo por personas independientes del área revisada (por ejemplo, la función de auditoría interna, un gestor independiente o una organización externa especializada en dichas revisiones). Las personas que realicen estas revisiones deberían tener la competencia adecuada. Persona que lleve a cabo las revisiones debería no estar en línea de autoridad para asegurar que tiene la independencia para hacer una evaluación.

Los resultados de revisiones independientes se deberían comunicar a la dirección que inició revisiones y, si procede, a la alta dirección. Estos registros se deberían mantener.

Si las revisiones independientes identifican que el enfoque y aplicación de la organización para gestionar seguridad de información son inadecuados [por ejemplo, los objetivos y requisitos documentados no se cumplen o no se ajustan a la dirección de seguridad de la información establecida en política de seguridad de la información y en políticas de temas específicos (ver 5.1)], la dirección debería iniciar acciones correctivas.

Además de revisiones independientes periódicas, la organización debería considerar la realización de revisiones independientes cuando:

a) leyes y reglamentos que afectan a la organización cambian;

b) incidentes significativos se produzcan;

c) la organización inicia un nuevo negocio o cambia un negocio actual;

d) la organización comienza a utilizar un nuevo producto o servicio, o cambia el uso de un producto o servicio actual;

e) la organización cambia los controles y procedimientos de seguridad de la información de forma significativa.

Otra información

Las normas ISO/IEC 27007 e ISO/IEC TS 27008 proporcionan guía para llevar a cabo revisiones independientes.

5.36 Cumplimiento de políticas, reglas y normas de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem

Control

Cumplimiento de política de seguridad de la información de la organización, políticas específicas de cada tema, reglas y normas se debería revisar regularmente.

Propósito

Garantizar que seguridad de la información se aplique y funcione de acuerdo con política de seguridad de la información de la organización, políticas específicas del tema, reglas y normas.

Guía

Los gestores, propietarios de servicios, productos o información deberían identificar cómo revisar que se cumplen requisitos de seguridad de la información definidos en política de seguridad de la información, políticas específicas del tema, reglas, normas y otras regulaciones aplicables. Se deberían considerar herramientas automáticas de medición e información para una revisión periódica eficaz.

Si se detecta algún incumplimiento como resultado de revisión, directivos deberían:

a) identificar causas de incumplimiento;

b) evaluar la necesidad de medidas correctoras para lograr la conformidad;

c) aplicar medidas correctoras adecuadas;

d) revisar medidas correctoras adoptadas para verificar su eficacia e identificar cualquier deficiencia o punto débil.

Los resultados de revisiones y acciones correctivas llevadas a cabo por gestores, propietarios de servicios, productos o información se deberían registrar y estos registros se deberían mantener. Los gestores deberían informar de resultados a personas que realizan revisiones independientes (ver 5.35) cuando tenga lugar una revisión independiente en el ámbito de su responsabilidad.

Las acciones correctivas se deberían completar de manera oportuna según el riesgo. Si no se completan para la siguiente revisión programada, avances se deberían abordar al menos en esa revisión.

Otros datos

La supervisión operativa del uso de sistema se trata en 8.15, 8.16 y 8.17.

5.37 Procedimientos operativos documentados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Control

Los procedimientos operativos de instalaciones de procesamiento de información deberían estar documentados y a disposición de personal que los necesite.

Propósito

Garantizar el funcionamiento correcto y seguro de instalaciones de tratamiento de información.

Guía

Se deberían preparar procedimientos documentados para actividades operativas de organización asociadas a seguridad de información, por ejemplo:

a) cuando la actividad se debería realizar de la misma manera por muchas personas;

b) cuando la actividad se realiza raramente y próxima vez que se realice es probable que se olvidó el procedimiento;

c) cuando la actividad es nueva y presenta un riesgo si no se realiza correctamente;

d) antes de entregar la actividad al nuevo personal.

e) Los procedimientos operativos deberían especificar:

f) las personas responsables;

g) la instalación y configuración seguras de sistemas;

h) procesamiento y tratamiento de información, tanto automatizado como manual;

i) copia de seguridad (ver 8.13) y la capacidad de recuperación;

j) requisitos de programación, incluyendo interdependencias con otros sistemas;

k) instrucciones para tratar errores u otras condiciones excepcionales [por ejemplo, restricciones en uso de programas de utilidad (ver 8.18)], que pueden surgir durante ejecución del trabajo;

l) contactos de apoyo y escalada, incluyendo contactos de apoyo externo en caso de dificultades operativas o técnicas inesperadas;

m) instrucciones de manipulación de los medios de almacenamiento (ver 7.10 y 7.14);

n) procedimientos de reinicio y recuperación de sistema para su uso en caso de fallo de este;

o) la gestión de información de pista de auditoría y de registro de sistema (ver 8.15 y 8.17) y sistemas de vigilancia por vídeo (ver 7.4);

p) procedimientos de control, como capacidad, rendimiento y seguridad (ver 8.6 y 8.16);

q) instrucciones de mantenimiento.

Se deberían revisar y documentar los procedimientos operativos documentados cuando sea necesario. Los cambios en procedimientos operativos documentados se deberían autorizar. Cuando sea técnicamente posible, los sistemas de información se deberían gestionar de forma coherente, usando los mismos procedimientos, herramientas y utilidades.

Otra información

Sin información.

6 Controles de personas

6.1 Control

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control

La comprobación de antecedentes de todos los candidatos al personal se debería realizar antes de incorporar a la organización y de forma continua, teniendo en cuenta leyes, reglamentos y ética aplicables y ser proporcional a los requisitos del negocio, clasificación de información a que se va a acceder y riesgos percibidos.

Propósito

Garantizar que todo el personal es elegible y adecuado para las funciones para las que se le considera y que sigue siendo elegible y adecuado durante su empleo.

Guía

Se debería realizar un proceso de selección para todo el personal, incluyendo a este a tiempo completo, parcial y trabajo temporal. En que estas personas se contratan a través de proveedores de servicios, los requisitos de selección se deberían incluir en acuerdos contractuales entre la organización y proveedores.

La información sobre todos los candidatos que se están considerando para puestos dentro de la organización se debería recopilar y manejar teniendo en cuenta cualquier legislación apropiada existente en la jurisdicción pertinente. En algunas jurisdicciones, se puede exigir legalmente a la organización que informe de antemano a los candidatos sobre actividades de selección.

La verificación debería tener en cuenta toda la legislación pertinente en materia de privacidad, protección de la información personal, empleo y debería incluir lo siguiente:

a) disponibilidad de referencias satisfactorias (por ejemplo, referencias empresariales y personales);

b) una verificación (para comprobar la integridad y exactitud) del currículum vitae del solicitante;

c) confirmación de las cualificaciones académicas y profesionales solicitadas;

d) verificación independiente de identidad (por ejemplo, pasaporte u otro documento aceptable expedido por autoridades competentes);

e) una verificación más detallada, como revisión del crédito o de antecedentes penales si el candidato asume un papel crítico.

En que se contrata a una persona para una función específica de seguridad de la información, la organización se debería asegurar de que el candidato:

a) tiene competencia necesaria para desempeñar la función de seguridad;

b) se puede confiar en que asumirá la función, especialmente si ésta es crítica para la organización.

En que un puesto de trabajo ya sea en el momento del nombramiento inicial o de promoción, implique que la persona tenga acceso a instalaciones de procesamiento de información y, en particular, si éstas implican el manejo de información confidencial (por ejemplo, información financiera, información personal o información sanitaria), la organización debería considerar también la posibilidad de realizar verificaciones más detalladas.

Procedimientos deberían definir criterios y limitaciones de revisiones de verificación (por ejemplo, quién es elegible para examinar a las personas, cómo, cuándo y por qué se llevan a cabo las revisiones de verificación).

Situaciones en que la verificación no se pueda completar a tiempo, se debería aplicar controles de mitigación hasta que la revisión haya finalizado, por ejemplo:

a) retraso en la incorporación;

b) retraso en el despliegue de los activos de la empresa;

c) incorporación con acceso reducido;

d) cese de relación laboral.

Los controles de verificación se deberían repetir periódicamente para confirmar la idoneidad permanente del personal, en función de la criticidad de la función de una persona.

Otra información

Sin información.

6.2 Términos y condiciones de trabajo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control

Los acuerdos contractuales de empleo deberían establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.

Propósito

Asegurar de que el personal entiende sus responsabilidades en materia de seguridad de la información para las funciones para las que se considera.

Guía

Las obligaciones contractuales para el personal deberían tener en cuenta política de seguridad de la información de la organización y políticas temáticas pertinentes. Además, se pueden aclarar y declarar los siguientes puntos:

a) acuerdos de confidencialidad o no divulgación que el personal al que se da acceso a información confidencial debería firmar antes de que se dé acceso a información y a otros activos asociados (ver 6.6);

b) responsabilidades y derechos legales [por ejemplo, en relación con leyes de derechos de autor o legislación de protección de datos (ver 5.32 y 5.34)];

c) responsabilidades en clasificación de información y gestión de la información de la organización y otros activos asociados, instalaciones de procesamiento de la información y servicios de información manejados por el personal (ver 5.9 a 5.13);

d) responsabilidades en el tratamiento de información recibida de las partes interesadas;

e) medidas que se tomarán si el personal hace caso omiso de los requisitos de seguridad de la organización (ver 6.4).

Se deberían comunicar las funciones y responsabilidades en materia de seguridad de información a candidatos durante el proceso previo a la contratación.

La organización debería asegurar que el personal acepta los términos y condiciones relativos a la seguridad de información. Estos términos y condiciones se deberían apropiar para la naturaleza y grado de acceso que tendrán a activos de la organización asociados a sistemas y servicios de información. Términos y condiciones relativos a seguridad de la información se deberían revisar cuando cambien las leyes, reglamentos, política de seguridad de la información o políticas de temas específicos.

Cuando corresponda, las responsabilidades contenidas en las condiciones de empleo deberían continuar durante un período definido después de finalización de empleo (ver 6.5).

Otra información

Un código de conducta se puede usar para establecer las responsabilidades del personal en materia de seguridad de la información en lo que respecta a la confidencialidad, la protección de PII, la ética, el uso adecuado de información de la organización y otros activos asociados, así como prácticas de reputación que espera la organización.

Se puede requerir a una parte externa, con que el personal del proveedor está asociado, que celebre acuerdos contractuales en nombre del individuo contratado.

Si la organización no es una entidad legal y no tiene empleados, el equivalente de acuerdo contractual, términos y condiciones se pueden considerar en línea con la guía de este control.

6.3 Concientización, educación y capacitación en seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control

El personal de la organización y partes interesadas pertinentes deberían recibir una concientización, educación y formación adecuadas en materia de seguridad de la información, así como actualizaciones periódicas de política de seguridad de la información de la organización y de políticas y procedimientos específicos, según sea pertinente para su función laboral.

Propósito

Garantizar que el personal, partes interesadas pertinentes conozcan y cumplan sus responsabilidades en materia de seguridad de la información.

Guía

Generalidades

Se debería establecer un programa de concientización, educación y formación en materia de seguridad de información en consonancia con política de seguridad de la información de la organización, políticas específicas de cada tema y procedimientos pertinentes en materia de seguridad de la información, teniendo en cuenta la información de la organización que se deberían proteger y controlar la seguridad de la información que se aplicó para protegerla.

La concientización, educación y formación en materia de seguridad de la información deberían tener lugar periódicamente. La concientización, educación y formación iniciales se pueden aplicar a personal nuevo y a que se trasladan a nuevos puestos o funciones con requisitos de seguridad de la información sustancialmente diferentes.

La comprensión del personal se debería evaluar al final de una actividad de sensibilización, educación o formación para comprobar la transferencia de conocimientos y eficacia de programa de sensibilización, educación y formación.

Concientización

Un programa de concientización sobre seguridad de la información debería tener como objetivo que el personal sea consciente de sus responsabilidades en materia de seguridad de la información y de los medios con los que se cumplen dichas responsabilidades.

El programa de sensibilización se debería planificar teniendo en cuenta las funciones del personal de la organización, incluyendo el personal interno y externo (por ejemplo, consultores externos, personal de los proveedores). Actividades del programa de concientización se deberían programar a lo largo del tiempo, preferiblemente de forma regular, para que actividades se repitan y abarquen a nuevo personal. También se deberían basar en lecciones aprendidas de incidentes de seguridad de información.

El programa de concientización debería incluir una serie de actividades de sensibilización a través de canales físicos o virtuales apropiados, como campañas, folletos, carteles, boletines, sitios Web, sesiones informativas, sesiones informativas, módulos de aprendizaje y correos electrónicos.

La concientización sobre seguridad de la información debería abarcar aspectos generales como:

a) compromiso de la dirección con seguridad de la información en toda la organización;

b) necesidades de conocimiento y cumplimiento de normas y obligaciones de seguridad de la información aplicables, teniendo en cuenta política de seguridad de la información y políticas, normas, leyes, estatutos, reglamentos, contratos y acuerdos específicos;

c) responsabilidad personal por propias acciones e inacciones y responsabilidades generales para asegurar o proteger información perteneciente a la organización y a las partes interesadas;

d) procedimientos básicos de seguridad de la información [por ejemplo, notificación de eventos de seguridad de la información (6.8)] y controles básicos [por ejemplo, seguridad de las contraseñas (5.17)];

e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre cuestiones de seguridad de la información, incluyendo material adicional de concientización sobre seguridad de la información.

Educación y formación

La organización debería identificar, preparar y poner en práctica un plan de formación adecuado para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y conocimientos específicos. Los equipos técnicos deberían tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios. Si faltan habilidades, la organización debería tomar medidas y adquirirlas.

El programa de educación y formación deberían contemplar diferentes formas [por ejemplo, conferencias o autoestudios, ser tutelado por personal experto o consultores (formación en el puesto de trabajo), rotar a los miembros del personal para que sigan diferentes actividades, contratar a personas ya capacitadas y contratar consultores]. Puede usar diferentes medios de impartición, incluyendo formación presencial, a distancia, a través de la Web, formación autodidacta y otras. El personal técnico debería mantener sus conocimientos al día suscribiéndose a boletines y revistas o asistiendo a conferencias y eventos destinados a la mejora técnica y profesional.

Otra información

Al momento de elaborar un programa de concientización, es importante no solo de debería centrar en el “qué” y “cómo”, sino también en el “por qué”, en que sea posible. Es importante que el personal entienda el objetivo de seguridad de la información y efecto potencial, positivo y negativo, de su propio comportamiento en la organización.

La concientización, educación y formación en materia de seguridad de la información pueden formar parte de otras actividades, o llevar a cabo en colaboración con ellas, por ejemplo, la formación en materia de gestión general de información, ICT, seguridad, privacidad o seguridad.

6.4 Proceso disciplinario

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_ security	#Governance_and_ Ecosystem

Control

Se debería formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

Propósito

Garantizar que el personal y otras partes interesadas pertinentes entiendan las consecuencias de violación de política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas pertinentes que cometieron violación.

Guía

El proceso disciplinario no se debería iniciar sin la comprobación previa de que se produjo una violación de política de seguridad de la información (ver 5.28).

El proceso disciplinario formal debería prever una respuesta gradual que tenga en cuenta factores como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad de incumplimiento y sus consecuencias;

b) si la infracción fue intencionada (dolosa) o no intencionada (accidental);

c) si se trata de una primera o reiterada infracción;

d) si el infractor recibió o no la formación adecuada.

La respuesta debería tener en cuenta requisitos legales, reglamentarios, contractuales y empresariales pertinentes, así como otros factores según sea necesario. El proceso disciplinario también se debería usar como elemento disuasorio para evitar que el personal y otras partes interesadas pertinentes infrinjan política de seguridad de la información, políticas específicas del tema y procedimientos de seguridad de la información. Violaciones deliberadas de política de seguridad de la información pueden requerir acciones inmediatas.

Otra información

En la medida de lo posible, la identidad de las personas sujetas a medidas disciplinarias se debería proteger de acuerdo con los requisitos aplicables.

Cuando los individuos demuestran un comportamiento excelente en materia de seguridad de la información, se pueden recompensar para promover seguridad de la información y fomentar el buen comportamiento.

6.5 Responsabilidades tras el cese o cambio de empleo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security #Asset_ management	#Governance_and_ Ecosystem

Control

Las responsabilidades y obligaciones en materia de seguridad de la información que siguen siendo válidas tras terminación o el cambio de empleo se deberían definir, aplicar y comunicar al personal pertinente y a otras partes interesadas.

Propósito

Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos.

Guía

El proceso para gestionar la terminación o cambio de empleo debería definir qué responsabilidades y deberes de seguridad de la información deberían seguir siendo válidos después de la terminación o cambio. Esto puede incluir confidencialidad de información, propiedad intelectual y otros conocimientos obtenidos, así como responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (ver 6.6). Responsabilidades y deberes que siguen siendo válidos después de la terminación de empleo o de contrato deberían estar contenidos en condiciones de empleo (ver 6.2), contrato o acuerdo del individuo. Otros contratos o acuerdos que continúen durante un período definido después de finalización de empleo de individuo también pueden contener responsabilidades de seguridad de información.

Los cambios de responsabilidad o empleo se deberían gestionar como cese de responsabilidad o empleo actual combinado con el inicio de nueva responsabilidad o empleo.

Las funciones y responsabilidades en materia de seguridad de la información de cualquier persona que abandone o cambie de puesto de trabajo se deberían identificar y transferir a otra persona.

Se debería establecer un proceso para comunicación de cambios y de procedimientos operativos al personal, a otras partes interesadas y a personas de contacto pertinentes (por ejemplo, a los clientes y proveedores).

Un proceso de cese o cambio de empleo se debería aplicar también al personal externo (por ejemplo, a los proveedores) cuando se produce un cese del personal, de contrato o del puesto de trabajo con la organización o cuando se produce un cambio de puesto de trabajo dentro de la organización.

Otra información

En muchas organizaciones, la función de recursos humanos suele ser responsable de proceso global de cese y trabaja junto con el responsable de la persona que pasa a serlo para gestionar aspectos de seguridad de la información de procedimientos pertinentes. En caso del 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 parte externa.

6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_ Ecosystem

Control

Los acuerdos de confidencialidad o de no divulgación que reflejan las necesidades de la organización en materia de protección de información se deberían identificar, documentar, revisar y firmar regularmente por personal y otras partes interesadas pertinentes.

Propósito

Mantener la confidencialidad de la información a la que puede acceder el personal o partes externas.

Guía

Los acuerdos de confidencialidad o no divulgación deberían abordar el requisito de proteger información confidencial usando términos exigibles legalmente. Los acuerdos de confidencialidad o no divulgación son aplicables a partes interesadas y personal de la organización. Sobre la base de requisitos de seguridad de información de una organización, términos de acuerdos se deberían determinar teniendo en cuenta el tipo de información que se manejará, su nivel de clasificación, su uso y el acceso permitido por la otra parte. Para identificar requisitos de acuerdos de confidencialidad o no divulgación, se deberían considerar los siguientes elementos:

a) una definición de la información que se debería proteger (por ejemplo, información confidencial);

b) la duración prevista de un acuerdo, incluyendo casos en que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información se haga pública;

c) las acciones requeridas cuando se termina un acuerdo;

d) las responsabilidades y acciones de firmantes para evitar divulgación de información no autorizada;

e) la propiedad de información, secretos comerciales, propiedad intelectual y su relación con la protección de información confidencial;

f) el uso permitido de la información confidencial y derechos del firmante a usar información;

g) el derecho a auditar y supervisar las actividades que implican información confidencial para circunstancias muy delicadas;

h) el proceso de notificación y denuncia de la divulgación no autorizada o de fuga de información confidencial;

i) las condiciones de devolución o destrucción de información al finalizar el acuerdo;

j) las acciones previstas en caso de incumplimiento del acuerdo.

La organización debería tener en cuenta el cumplimiento de acuerdos de confidencialidad y no divulgación para la jurisdicción a que se aplican (ver 5.31, 5.32, 5.33, 5.34).

Los requisitos de acuerdos de confidencialidad y no divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

Otra información

Los acuerdos de confidencialidad y no divulgación protegen información de la organización e informan a los firmantes de su responsabilidad de proteger, usar, divulgar información de forma responsable y autorizada.

6.7 Trabajo a distancia

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection

Control

Las medidas de seguridad se deberían aplicar cuando el personal trabaja a distancia para proteger información a que se accede, procesa o almacena fuera de las instalaciones de la organización.

Propósito

Garantizar seguridad de la información cuando el personal trabaja a distancia.

Guía

El trabajo a distancia se produce cuando el personal de la organización trabaja desde un lugar fuera de las instalaciones de la organización, accediendo a información ya sea de manera impresa o electrónicamente a través de equipos ICT. Los entornos de trabajo a distancia incluyen los denominados “teleworking[2]”, “telecommuting[3]”, “flexible workplace[4]”, “virtual work environments[5]” y “remote maintenance[6]”.

NOTA Es posible que no se puedan aplicar todas las recomendaciones de esta guía debido a la legislación y los reglamentos locales de las distintas jurisdicciones.

2 Del inglés teleworking: *teletrabajo*.

3 Del inglés telecommuting: *teletrabajo*.

4 Del inglés flexible workplace: *centro de trabajo, lugar de trabajo o puesto de trabajo flexible*.

5 Del inglés virtual work environments: *entorno de trabajo virtual*.

6 Del inglés remote maintenance: *mantenimiento a distancia, mantenimiento remoto o telemantenimiento*.

Las organizaciones que permiten actividades de trabajo a distancia deberían emitir una política específica sobre trabajo a distancia que defina condiciones y restricciones pertinentes. Cuando se considere aplicable, se deberían tener en cuenta los siguientes temas:

a) la seguridad física existente o propuesta del lugar de trabajo a distancia, teniendo en cuenta la seguridad física del lugar y entorno local, incluyendo diferentes jurisdicciones en que se encuentra el personal;

b) normas y mecanismos de seguridad para el entorno físico a distancia, como armarios con cerradura, transporte seguro entre ubicaciones y normas para el acceso a distancia, escritorio despejado, impresión, eliminación de información, otros activos asociados y notificación de eventos de seguridad de la información (ver 6.8);

c) entornos físicos de trabajo a distancia previstos;

d) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a sistemas de la organización, sensibilidad de información a que se va a acceder y que va a pasar por el enlace de comunicación y sensibilidad de sistemas y aplicaciones;

e) el uso de acceso remoto, como acceso a escritorios virtuales, que permite el procesamiento y almacenamiento de información en equipos de propiedad privada;

f) la amenaza de acceso no autorizado a información o a recursos por parte de otras personas en el lugar de trabajo a distancia (por ejemplo, familiares y amigos);

g) la amenaza de acceso no autorizado a información o recursos por parte de otras personas en lugares públicos;

h) el uso de las redes domésticas y de redes públicas y requisitos o restricciones en configuración de servicios de redes inalámbricas;

i) uso de medidas de seguridad, como cortafuegos y protección contra “malware”;

j) mecanismos seguros para desplegar e inicializar sistemas a distancia;

k) mecanismos seguros de autenticación y habilitación de privilegios de acceso teniendo en cuenta la vulnerabilidad de mecanismos de autenticación de factor único en que se permite el acceso remoto a la red de la organización.

Directrices y medidas a considerar deberían incluir:

a) la provisión de equipos y mobiliario de almacenamiento adecuados para actividades de trabajo a distancia, en que no se permite uso de equipos de propiedad privada que no estén bajo control de la organización;

b) una definición de trabajo permitido, clasificación de información que puede poseer y sistemas y servicios internos a que el trabajador a distancia está autorizado a acceder;

c) la provisión de formación para los que trabajan a distancia y para los que prestan apoyo. Esto debería incluir cómo llevar a cabo los negocios de forma segura mientras se trabaja a distancia;

d) el suministro de equipos de comunicación adecuados, incluyendo métodos para asegurar acceso remoto, como requisitos de bloqueo de pantalla de dispositivo y temporizadores de inactividad; habilitación de monitoreo de ubicación de dispositivo; instalación de capacidades de borrado remoto;

e) seguridad física;

f) normas y orientaciones sobre acceso de familias 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 copia de seguridad y continuidad de la actividad;

j) auditoría y supervisión de seguridad;

k) revocación de autoridad, derechos de acceso y devolución de los equipos cuando finalicen las actividades de trabajo a distancia.

Otra información

Sin información.

6.8 Informe de eventos de seguridad de la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence

Control

La organización debería proporcionar un mecanismo para que el personal informe de los eventos de seguridad de la información observados o sospechosos a través de canales apropiados de manera oportuna.

Propósito

Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que se puedan identificar por el personal.

Guía

Todo el personal y usuarios se deberían concientizar de su responsabilidad de informar de los eventos de seguridad de la información lo antes posible para prevenir o minimizar el efecto de incidentes de seguridad de la información.

También deberían conocer el procedimiento de notificación de sucesos relacionados con seguridad de la información y de contacto al que se debería notificar los sucesos. El mecanismo de notificación debería ser lo más fácil, accesible y disponible posible. Eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades.

Situaciones que se deberían considerar para la notificación de eventos de seguridad de la información incluyen:

a) controles de seguridad de la información ineficaces;

b) violación de las expectativas de confidencialidad, integridad o disponibilidad de la información;

c) errores humanos;

d) incumplimiento de política de seguridad de información, políticas específicas del tema o normas aplicables;

e) violaciones de medidas de seguridad física;

f) cambios en sistema que no pasaron por el proceso de gestión de cambios;

g) mal funcionamiento u otro comportamiento anómalo de sistema de “software” o “hardware”;

h) violaciones de acceso;

i) vulnerabilidades;

j) sospecha de infección por malware.

Se debería aconsejar al personal y a usuarios que no intenten probar las presuntas vulnerabilidades de seguridad de la información. El probar vulnerabilidades se puede interpretar como un posible mal uso de sistema y también puede causar daños al sistema o servicio de información y puede corromper u ocultar las pruebas digitales. En última instancia, esto puede dar lugar a una responsabilidad legal para la persona que realiza las pruebas.

Otra información

Ver norma ISO/IEC 27035 para más información.

7 Controles físicos

7.1 Perímetros de seguridad física

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Los perímetros de seguridad se deberían definir y usar para proteger áreas que contienen información y otros activos asociados.

Propósito

Impedir el acceso físico no autorizado, daños e interferencias en información de la organización y otros activos asociados.

Guía

Las siguientes directrices se deberían considerar y aplicar en que se apropie a perímetros de seguridad física:

a) definir perímetros de seguridad, emplazamiento y solidez de cada uno de perímetros de acuerdo con requisitos de seguridad de la información relacionados con activos dentro del perímetro;

b) tener perímetros físicamente sólidos para un edificio o sitio que contenga instalaciones de procesamiento de información (por ejemplo, no debería haber huecos en el perímetro ni zonas en que se pueda producir fácilmente un robo). Tejados, paredes, techos y suelos exteriores del recinto deberían ser de construcción sólida y todas las puertas exteriores deberían estar convenientemente protegidas contra acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). Puertas y ventanas deberían estar cerradas con llave cuando no estén vigiladas y se debería considerar la posibilidad de instalar protecciones externas en las ventanas, especialmente a nivel del suelo; también se deberían considerar los puntos de ventilación;

c) establecer el nivel de resistencia requerido de acuerdo con normas adecuadas, alarma, control y comprobación de todas las puertas cortafuegos de un perímetro de seguridad junto con paredes. Deberían funcionar a prueba de fallos.

Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de locales de la organización y de instalaciones de procesamiento de información.

Una zona segura puede ser una oficina con cerradura o varias salas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. La organización debería considerar la posibilidad de contar con medidas de seguridad física que se puedan reforzar en situaciones de mayor amenaza.

7.2 Acceso físico

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection

Control

Las zonas seguras deberían estar protegidas por controles de entrada y puntos de acceso adecuados.

Propósito

Garantizar solo acceso físico autorizado a información de la organización y otros activos asociados se produce.

Guía

Generalidades

Los puntos de acceso, así como las zonas de entrega y carga y otros puntos en que pueden entrar personas no autorizadas, deberían estar controlados y, si es posible, aislados de las instalaciones de procesamiento de información para evitar acceso no autorizado.

Se deberían tener en cuenta las siguientes directrices:

a) restringir acceso a los lugares y edificios únicamente al personal autorizado. El proceso de gestión de los derechos de acceso a áreas físicas debería incluir provisión, revisión periódica, actualización y revocación de las autorizaciones (ver 5.18);

b) mantener y supervisar de forma segura un libro de registro físico o una pista de auditoría electrónica de todos accesos y proteger todos los registros (ver 5.33) e información sensible de autenticación;

c) establecer, aplicar un proceso y mecanismos técnicos para la gestión de acceso a áreas en que se procesa o almacena 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 debería considerar la posibilidad de usar dobles puertas de seguridad para acceso a zonas sensibles;

d) establecer una zona de recepción vigilada por personal u otros medios para controlar acceso físico al lugar o al edificio;

e) inspeccionar y examinar las pertenencias personales del personal y de interesados a entrada y a salida;

NOTA Pueden existir legislaciones y normativas locales sobre la posibilidad de inspeccionar los objetos personales.

f) exigir a todo el personal y a las partes interesadas que lleven algún tipo de identificación visible y que avisen inmediatamente al personal de seguridad si se encuentran con visitantes sin escolta y con cualquier persona que no lleve una identificación visible. Se debería estudiar la posibilidad de usar distintivos fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes;

g) conceder al personal de proveedores un acceso restringido a zonas seguras o a instalaciones de tratamiento de información solo en que sea necesario. Este acceso se debería autorizar y supervisar;

h) prestar especial atención a la seguridad de acceso físico en caso de edificios que albergan bienes para múltiples organizaciones;

i) diseñar medidas de seguridad física de manera que se puedan reforzar cuando aumente la probabilidad de incidentes físicos;

j) asegurar otros puntos de entrada, como salidas de emergencia, contra acceso no autorizado;

k) establecer un proceso de gestión de llaves para garantizar la gestión de llaves físicas o información de autenticación (por ejemplo, códigos de cerraduras, cerraduras de combinación de oficinas, salas e instalaciones como armarios de llaves) y garantizar un libro de registro o una auditoría anual de las llaves y que se controle acceso a llaves físicas o a información de autenticación (ver 5.17 para obtener guía sobre información de autenticación).

Visitantes

Se deberían tener en cuenta las directrices siguientes:

a) autenticar identidad de visitantes por un medio adecuado;

b) registrar fecha, hora de entrada y salida de visitantes;

c) conceder acceso a los visitantes solo para fines específicos, autorizados y con instrucciones sobre requisitos de seguridad de zona y sobre procedimientos de emergencia;

d) supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

Zonas de entrega, carga y material entrante

Se deberían tener en cuenta las siguientes directrices:

a) restringir acceso a zonas de entrega y carga desde el exterior del edificio al personal identificado y autorizado;

b) diseñar zonas de entrega y carga de manera que entregas se puedan cargar y descargar sin que el personal de entrega acceda sin autorización a otras partes del edificio;

c) asegurar las puertas exteriores de zonas de entrega y carga cuando se abran las puertas de zonas restringidas;

d) inspeccionar y examinar entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que salgan de zonas de entrega y carga;

e) registrar entregas entrantes de acuerdo con procedimientos de gestión de activos (ver 5.9 y 7.10) a la entrada del centro;

f) separar físicamente envíos entrantes y salientes, en que sea posible;

g) inspeccionar entregas entrantes para detectar indicios de manipulación en camino. Si se descubren manipulaciones, se debería comunicar inmediatamente a personal de seguridad.

Otra información

Sin información.

7.3 Aseguramiento de oficinas, salas e instalaciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Se deberían diseñar y aplicar seguridad física de oficinas, salas e instalaciones.

Propósito

Impedir acceso físico no autorizado, daños e interferencias en información de la organización y otros activos asociados en oficinas, salas e instalaciones.

Guía

Para asegurar despachos, salas e instalaciones se deberían tener en cuenta las directrices siguientes:

a) situar instalaciones críticas para evitar acceso de público;

b) garantizar que los edificios sean discretos y den una indicación mínima de su finalidad, en que proceda, sin signos evidentes, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información;

c) configurar instalaciones para evitar que información o actividades confidenciales sean visibles y audibles desde el exterior. También se debería considerar el blindaje electromagnético, según proceda;

d) no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen la ubicación de instalaciones de procesamiento de información confidencial.

Otra información

Sin información.

7.4 Supervisión de seguridad física

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

Control

Las instalaciones deberían estar vigiladas continuamente para evitar acceso físico no autorizado.

Propósito

Detectar e impedir el acceso físico no autorizado.

Guía

Las instalaciones físicas deberían estar controladas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de vigilancia por vídeo, como televisión en circuito cerrado y programas informáticos de gestión de información sobre seguridad física ya sean gestionados internamente o por un proveedor de servicios de vigilancia.

El acceso a edificios que albergan sistemas críticos debería estar vigilado continuamente para detectar accesos no autorizados o comportamientos sospechosos al:

a) instalar sistemas de vigilancia por vídeo, como un circuito cerrado de televisión, para ver y grabar acceso a las zonas sensibles dentro y fuera de los locales de una organización;

b) instalar, de acuerdo con normas aplicables pertinentes y comprobar periódicamente los detectores de contacto, sonido o movimiento para activar una alarma de intrusión, como, por ejemplo:

   1) instalar detectores de contacto que activen una alarma cuando se haga o se rompa un contacto en cualquier lugar en que se pueda hacer o romper un contacto (como ventanas, puertas y debajo de objetos) para usarlo como alarma de pánico;

   2) instalar detector de movimiento basados en tecnología de infrarrojos que activan una alarma cuando un objeto pasa por su campo de visión;

   3) instalar sensores sensibles al sonido de rotura de cristales que puedan servir para activar una alarma que alerte al personal de seguridad;

c) usar esas alarmas para cubrir todas las puertas exteriores y ventanas accesibles. Zonas desocupadas deberían estar alarmadas en todo momento; también se debería proporcionar cobertura para otras zonas (por ejemplo, salas de computadores o de comunicaciones).

El diseño de sistemas de vigilancia debería ser confidencial porque su divulgación puede facilitar los robos no detectados.

Los sistemas de vigilancia deberían estar protegidos contra acceso no autorizado para evitar que personas no autorizadas accedan a información de vigilancia, como transmisiones de vídeo o que sistemas se desactiven a distancia.

El panel de control de sistema de alarma debería estar situado en una zona alarmada y en el caso de alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que da la alarma. El panel de control y detectores deberían tener mecanismos a prueba de manipulaciones. El sistema se debería probar periódicamente para garantizar su funcionamiento, especialmente si sus componentes funcionan con baterías.

Cualquier mecanismo de supervisión y grabación se debería usar teniendo en cuenta leyes y normativas locales, incluida legislación sobre protección de datos y de información personal, especialmente en lo que respecta a supervisión del personal y a períodos de conservación de los vídeos grabados.

Otra información

Sin información.

7.5 Protección contra amenazas físicas y medioambientales

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Se debería diseñar y aplicar una protección contra amenazas físicas y medioambientales, como catástrofes naturales y otras amenazas físicas, intencionadas o no, a infraestructuras.

Propósito

Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y ambientales.

Guía

Las evaluaciones de riesgo para identificar las consecuencias potenciales de amenazas físicas y ambientales se deberían realizar antes de comenzar operaciones críticas en un sitio físico y a intervalos regulares. Se deberían aplicar los salvaguardias necesarios y supervisar los cambios en amenazas. Se debería obtener asesoramiento de especialistas sobre cómo gestionar riesgos derivados de amenazas físicas y medioambientales, como incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y otras formas de catástrofes naturales o provocadas por el ser humano.

Ubicación y construcción de instalaciones físicas debería 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.

Sobre la base de resultados de evaluación de riesgos, se deberían identificar amenazas físicas, medioambientales pertinentes y considerar los controles adecuados en los siguientes contextos, a modo de ejemplo:

a) incendio: instalación y configuración de sistemas capaces de detectar incendios en una fase temprana para enviar alarmas o activar sistemas de supresión de incendios con el fin de evitar daños por incendio a medios de almacenamiento y a sistemas de procesamiento de información relacionados. La supresión de incendios se debería realizar usando sustancia más adecuada en relación con el entorno (por ejemplo, gas en espacios confinados);

b) inundación: instalación de sistemas capaces de detectar la inundación en una fase temprana bajo los suelos de zonas que contienen medios de almacenamiento o sistemas de procesamiento de información. Bombas de agua o medios equivalentes deberían estar fácilmente disponibles en caso de que se produzca una inundación;

c) sobretensiones eléctricas: adoptar sistemas capaces de proteger tanto sistemas de información del servidor como del cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de dichos eventos;

d) explosivos y armas: realización de inspecciones aleatorias para detectar presencia de explosivos o armas en el personal, vehículos o mercancías que entran en instalaciones de tratamiento de información sensible.

Otros datos

Las cajas fuertes u otras formas de almacenamiento seguro pueden proteger información almacenada en ellas contra catástrofes como un incendio, terremoto, inundación o explosión.

Las organizaciones pueden tener en cuenta los conceptos de prevención de la delincuencia a través del diseño ambiental a la hora de diseñar controles para asegurar su entorno y reducir amenazas urbanas. Por ejemplo, en lugar de usar bolardos, estatuas o elementos de agua pueden servir tanto de elemento como de barrera física.

7.6 Trabajo en zonas seguras

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Se deberían diseñar y aplicar medidas de seguridad para trabajar en zonas seguras.

Propósito

Proteger información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Guía

Las medidas de seguridad para trabajar en zonas seguras se deberían aplicar a todo el personal y abarcar todas las actividades que tengan lugar en zona segura.

Se deberían tener en cuenta las siguientes directrices:

a) hacer que el personal solo conozca la existencia de una zona segura, o actividades que se realizan en ella, en función de la necesidad de conocerla;

b) evitar trabajo no supervisado en zonas seguras, tanto por razones de seguridad como para reducir posibilidades de actividades maliciosas;

c) cerrar físicamente e inspeccionar de manera periódica zonas seguras vacías;

d) no permitir equipos de fotografía, vídeo, audio u otros equipos de grabación, como cámaras en dispositivos de usuarios, a menos que se autorice;

e) controlar adecuadamente el transporte y uso de dispositivos de usuarios en las zonas seguras;

f) publicar procedimientos de emergencia en un lugar fácilmente visible o accesible.

Otra información

Sin información.

7.7 Escritorio y pantalla despejados

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Control

Se deberían definir y aplicar adecuadamente normas claras para los papeles y medios de almacenamiento extraíbles y normas claras para pantallas de instalaciones de procesamiento de información.

Propósito

Reducir riesgos de acceso no autorizado, pérdida y daño de información en escritorios, pantallas y otros lugares accesibles durante y fuera del horario de trabajo.

Guía

La organización debería establecer y comunicar a todas las partes interesadas pertinentes una política específica sobre el tema de escritorios y pantallas transparentes.

Se deberían tener en cuenta las directrices siguientes:

a) guardar bajo llave información sensible o crítica de la empresa (por ejemplo, en papel o en medios de almacenamiento electrónico) (idealmente en una caja fuerte, armario u otra forma de mobiliario de seguridad) cuando no se necesite, especialmente cuando la oficina esté desocupada;

b) Proteger dispositivos de puntos finales de usuarios mediante cerraduras con llave u otros medios de seguridad cuando no se usen o estén desatendidos;

c) dejar los dispositivos terminales del usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación del usuario cuando estén desatendidos. Todos los computadores y sistemas deberían estar configurados con una función de tiempo de espera o de cierre de sesión automático;

d) hacer que el remitente recoja las salidas de las impresoras o dispositivos multifunción de forma inmediata. Uso de impresoras con una función de autentificación, para que los originadores sean los únicos que puedan obtener sus impresiones y solo cuando estén junto a la impresora;

e) almacenar de forma segura los documentos y medios de almacenamiento extraíbles que contengan información sensible y cuando ya no se necesiten, desecharlos mediante mecanismos de eliminación seguros;

f) establecer y comunicar normas y orientaciones para la configuración de ventanas emergentes en pantallas (por ejemplo, desactivar las nuevas ventanas emergentes del correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en una zona pública);

g) borrar la información sensible o crítica de pizarras y otros tipos de pantalla cuando ya no sea necesaria.

La organización debería contar con procedimientos al desalojar las instalaciones, incluyendo realización de un barrido final antes de la salida para garantizar que no se dejan atrás activos de la organización (por ejemplo, documentos caídos detrás de cajones o muebles).

Otra información

Sin información.

7.8 Ubicación y protección de equipos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

El equipo debería estar ubicado de forma segura y protegida.

Propósito

Reducir riesgos derivados de amenazas físicas y ambientales, de accesos y daños no autorizados.

Guía

Las siguientes directrices se deberían considerar para proteger el equipo:

a) situar equipos para minimizar acceso innecesario a zonas de trabajo y evitar acceso no autorizado;

b) situar, de manera prudente, las instalaciones de procesamiento de información que manejan datos sensibles para reducir el riesgo de que la información se observe por personas no autorizadas durante su uso;

c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales [por ejemplo, robo, incendio, explosivos, humo, agua (o fallos en el suministro de agua), polvo, vibraciones, efectos químicos, interferencias en suministro eléctrico, interferencias en comunicaciones, radiaciones electromagnéticas y vandalismo];

d) establecer directrices para comer, beber y fumar cerca de instalaciones de procesamiento de información;

e) controlar condiciones ambientales, como temperatura y humedad, para detectar condiciones que puedan afectar negativamente al funcionamiento de instalaciones de tratamiento de información;

f) aplicar protección contra el rayo en todos los edificios e instalar filtros de protección contra el rayo en todas las líneas eléctricas y de comunicaciones entrantes;

g) considerar uso de métodos especiales de protección, como membranas de teclado, para equipos en entornos industriales;

h) proteger equipos que procesan información confidencial para minimizar riesgo de fuga de información debido a emanación electromagnética;

i) separar físicamente las instalaciones de procesamiento de información gestionadas por la organización de las que no son.

Otra información

Sin información.

7.9 Seguridad de activos fuera de las instalaciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Los activos fuera de las instalaciones deberían estar protegidos.

Propósito

Para evitar pérdida, daño, robo o compromiso de dispositivos fuera del sitio e interrupción de operaciones de la organización.

Guía

Cualquier dispositivo usado fuera de instalaciones de la organización que almacene o procese información (por ejemplo, un dispositivo móvil), incluyendo dispositivos de propiedad de la organización y dispositivos de propiedad privada usados en nombre de la organización [‘bring your own device’ principle (BYOD)] necesita protección. El uso de estos dispositivos se debería autorizar por la dirección.

Para protección los dispositivos que almacenan o procesan, se deberían tener en cuenta las siguientes directrices información fuera de instalaciones de la organización:

a) no dejar desatendidos los equipos y soportes de almacenamiento que se lleven fuera de las instalaciones en lugares públicos y no seguros;

b) respetar instrucciones de fabricantes para proteger equipos en todo momento (por ejemplo, protección contra la exposición a fuertes campos electromagnéticos, agua, calor, humedad, polvo);

c) mantener un registro que defina la cadena de custodia de equipos, incluyendo al menos nombres y organizaciones de los responsables de equipos, cuando se transfieran equipos fuera de instalaciones entre diferentes personas o partes interesadas. Información que no necesita se transfiera con el activo se debería eliminar de forma segura antes de la transferencia;

d) exigir autorización para la retirada de equipos y soportes de locales de organización y llevar un registro de dichas retiradas para mantener una pista de auditoría, en que sea necesario y práctico, (ver 5.14);

e) proteger contra visualización de información en un dispositivo (por ejemplo, celular o computador portátil) en transporte público y riesgos asociados a la navegación por el hombro;

f) implementar monitoreo de ubicación y capacidad de borrar a distancia los dispositivos.

La instalación permanente de equipos fuera de los locales de la organización [como antenas y cajeros automáticos (ATM)] puede estar sujeta a un mayor riesgo de daños, robo o escuchas. Estos riesgos pueden variar considerablemente entre distintos lugares y se deberían tener en cuenta a la hora de determinar medidas más adecuadas. Se deberían tener en cuenta las siguientes directrices al momento de ubicar estos equipos fuera de las instalaciones de la organización:

a) vigilancia de seguridad física (ver 7.4);

b) protección contra las amenazas físicas y medioambientales (ver 7.5);

c) controles de acceso físico y antimanipulación;

d) controles de acceso lógico.

Otros datos

En 8.1 y 6.7 se pueden encontrar más información sobre otros aspectos de protección de equipos de almacenamiento y procesamiento de información y de dispositivos finales de usuarios.

7.10 Medios de almacenamiento

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Los soportes de almacenamiento se deberían gestionar a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y requisitos de manipulación de la organización.

Propósito

Garantizar solo la divulgación, modificación, eliminación o destrucción autorizada de la información en los soportes de almacenamiento.

Guía

Medios de almacenamiento extraíbles

Se deberían tener en cuenta las siguientes directrices para la gestión de los medios de almacenamiento extraíbles:

a) establecer una política específica sobre la gestión de los medios de almacenamiento extraíbles y comunicar dicha política específica a cualquier persona que utilice o maneje medios de almacenamiento extraíbles;

b) exigir la autorización para la retirada de los soportes de almacenamiento de la organización y mantener un registro de dichas retiradas con el fin de mantener una pista de auditoría, en que sea necesario y práctico;

c) almacenar todos los soportes de almacenamiento en un entorno seguro, de acuerdo con su clasificación de la información y protegerlos contra las amenazas ambientales (como el calor, la humedad, el campo electrónico o el envejecimiento), de acuerdo con las especificaciones de los fabricantes;

d) usar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles, si la confidencialidad o integridad de información son consideraciones importantes;

e) mitigar riesgo que los medios de almacenamiento se degraden mientras la información almacenada sigue siendo necesaria, transfiriendo la información a medios de almacenamiento nuevos antes de que sea ilegible;

f) almacenar varias copias de información valiosa en soportes de almacenamiento separados para reducir aún más riesgo de daños o pérdidas de información por casualidad;

g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) habilitar solo puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas digitales seguras (SD) y puertos de bus serie universal (USB)] si hay una razón organizativa para su uso;

i) usar medios de almacenamiento extraíbles en que sea necesario, controlar la transferencia de información a dichos medios de almacenamiento;

j) informar puede ser vulnerable al acceso no autorizado, uso indebido o a corrupción durante el transporte físico, por ejemplo, cuando se envían soportes de almacenamiento a través del servicio postal o de mensajería.

En este control, los soportes incluyen los documentos en papel. Transferir soportes físicos, aplique medidas de seguridad indicadas en el 5.14.

Reutilización o eliminación segura

Procedimientos para reutilización o eliminación segura de medios de almacenamiento se deberían establecer para minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Procedimientos para reutilización o eliminación segura de soportes de almacenamiento que contienen información confidencial deberían ser proporcionales a la sensibilidad de dicha información. Se deberían tener en cuenta los siguientes elementos:

a) borrar datos de forma segura o formatear el medio de almacenamiento antes de su reutilización (ver 8.10), si los medios de almacenamiento que contienen información confidencial se deberían reutilizar dentro de la organización;

b) eliminar de forma segura los soportes de almacenamiento que contengan información confidencial cuando ya no se necesiten (por ejemplo, destruyendo, triturando o borrando de forma segura el contenido);

c) disponer de procedimientos para identificar los artículos que pueden requerir una eliminación segura;

d) recoger y eliminar de soportes de almacenamiento ofrecen muchas organizaciones de servicios. Debería poner especial atención al seleccionar un proveedor externo adecuado con controles y experiencia adecuados;

e) registrar eliminación de elementos sensibles para mantener una pista de auditoría;

f) acumular soportes de almacenamiento para su eliminación, tener en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se convierta en sensible.

Se debería realizar una evaluación de riesgos en los dispositivos dañados que contengan datos sensibles para determinar si los artículos se deberían destruir físicamente en lugar de ser enviados para su reparación o desechados (ver 7.14).

Otra información

Cuando la información confidencial en los medios de almacenamiento no está encriptada, se debería considerar una protección física adicional de los medios de almacenamiento.

7.11 Servicios de apoyo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Control

Las instalaciones de procesamiento de información deberían estar protegidas contra cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.

Propósito

Evitar la pérdida, daño o puesta en peligro de información y otros activos asociados o interrupción de las operaciones de la organización debido al fallo e interrupción de servicios de apoyo.

Guía

Las organizaciones dependen de servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para apoyar sus instalaciones de procesamiento de información. Por lo tanto, la organización debería:

a) garantizar que los equipos que soportan servicios públicos están configurados, funcionan y se mantienen de acuerdo con las especificaciones del fabricante correspondiente;

b) garantizar que los servicios públicos se evalúen periódicamente en cuanto a su capacidad para satisfacer crecimiento de empresa e interacciones con otros servicios de apoyo;

c) garantizar que los equipos de apoyo a los servicios públicos se inspeccionen y prueben periódicamente para garantizar su correcto funcionamiento;

d) activar alarmas para detectar el mal funcionamiento de los servicios, si es necesario;

e) garantizar que las empresas de servicios públicos dispongan de varias alimentaciones con diversos encaminamientos físicos, si es necesario;

f) garantizar que los equipos que soportan los servicios públicos están en una red separada de instalaciones de procesamiento de información, si están conectadas a una red;

g) garantizar que los equipos que soportan los servicios públicos se conecten a Internet solo en que sea necesario y de forma segura.

Debería haber iluminación y comunicaciones de emergencia. Interruptores y válvulas de emergencia para cortar electricidad, agua, gas u otros servicios deberían estar situados cerca de salidas de emergencia o de salas de equipos. Detalles de contactos de emergencia se deberían registrar y estar disponibles para el personal en caso de que se produzca un apagón.

Otra información

Se puede obtener una redundancia adicional para la conectividad de red mediante múltiples rutas de más de un proveedor de servicios.

7.12 Seguridad de cableado

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

Control

Los cables que transportan energía, datos o servicios de información de apoyo deberían estar protegidos contra la interceptación, las interferencias o los daños.

Propósito

Evitar pérdida, daño, robo o puesta en peligro de información y otros activos asociados, así como interrupción de operaciones de la organización relacionadas con el cableado de alimentación y comunicaciones.

Guía

Se deberían considerar las siguientes directrices para la seguridad del cableado:

a) las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información deben ser subterráneas en la medida de lo posible, o deben estar 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) separación de cables de alimentación de los de comunicaciones para evitar interferencias;

c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:

   1) instalación de conductos blindados y salas 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 los paneles de conexión y a las salas de cables (por ejemplo, con llaves mecánicas o PIN);

   5) uso de cables de fibra óptica;

d) etiquetación de cables en cada extremo con suficientes detalles de origen y destino para permitir identificación física e inspección del cable.

Se debería solicitar asesoramiento de un especialista sobre cómo gestionar riesgos derivados de incidentes o mal funcionamiento del cableado.

Otra información

En algunas ocasiones, el cableado de alimentación y de telecomunicaciones son recursos compartidos por más de una organización que ocupa locales comunes.

7.13 Mantenimiento de equipo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

Control

Los equipos se deberían mantener correctamente para garantizar la disponibilidad, integridad y confidencialidad de información.

Propósito

Evitar pérdida, daño, robo o puesta en peligro de información y otros activos asociados, así como la interrupción de operaciones de la organización causada por la falta de mantenimiento.

Guía

Se deberían tener en cuenta las siguientes directrices para el mantenimiento de los equipos:

a) mantener el equipo de acuerdo con la frecuencia de servicio y las especificaciones recomendadas por el proveedor;

b) aplicar y seguir de un programa de mantenimiento por parte de la organización;

c) realizar reparaciones y el mantenimiento de equipos solo el personal de mantenimiento autorizado;

d) mantener un registro de todas las averías presuntas o reales y de todo mantenimiento preventivo y correctivo;

e) aplicar controles adecuados cuando se programe el mantenimiento de equipos, teniendo en cuenta si este mantenimiento lo realiza personal in situ o externo a la organización; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado;

f) supervisar al personal de mantenimiento cuando realizar mantenimiento in situ;

g) autorizar y controlar acceso para mantenimiento a distancia;

h) aplicar medidas de seguridad para activos fuera de locales (ver 7.9) si los equipos que contienen información se sacan de los locales para su mantenimiento;

i) cumplir con todos los requisitos de mantenimiento impuestos por el seguro;

j) inspeccionarlo para asegurar que no se manipuló que funciona correctamente, antes de volver a poner en funcionamiento el equipo después del mantenimiento,

k) aplicar medidas para eliminación segura o reutilización de los equipos (ver 7.14) si se determina que los equipos van a ser eliminados.

Otra información

Los equipos incluyen componentes técnicos de instalaciones de procesamiento de información, sistemas de alimentación ininterrumpida (UPS) y baterías, generadores de energía, alternadores y convertidores de energía, sistemas de detección de intrusión física y alarmas, detectores de humo, extintores, aire acondicionado y ascensores.

7.14 Eliminación segura o reutilización de equipos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

Control

Los equipos que contienen soportes de almacenamiento se deberían verificar para garantizar que cualquier dato sensible y “software” con licencia se eliminó o sobrescribió de forma segura antes de su eliminación o reutilización.

Propósito

Para evitar la fuga de información de los equipos que van a ser eliminados o reutilizados.

Guía

El equipo se debería verificar para asegurar que los medios de almacenamiento están contenidos o no antes de su eliminación o reutilización.

Los soportes de almacenamiento que contengan información confidencial o protegida por derechos de autor o información se deberían destruir físicamente o borrar o sobrescribir usando técnicas para que la información original no sea recuperable en lugar de usar la función de borrado estándar. Ver 7.10 para una guía detallada sobre eliminación segura de medios de almacenamiento y 8.10 para una guía sobre eliminación de la información.

Las etiquetas y marcas que identifican a la organización o que indican la clasificación, propietario, sistema o red, se deberían retirar antes de eliminarla, incluyendo reventa o donación a la beneficencia.

La organización debería considerar eliminación de controles de seguridad, como los de acceso o equipos de vigilancia, al final de contrato de arrendamiento o cuando se cambien de locales. Esto depende de factores como:

a) contrato de arrendamiento para devolver las instalaciones a su estado original;

b) minimización de riesgo de dejar sistemas con información sensible para el siguiente inquilino (por ejemplo, listas de acceso de usuarios, archivos de vídeo o imágenes);

c) la posibilidad de reutilizar controles en la siguiente instalación.

Otra información

Los equipos dañados que contienen medios de almacenamiento pueden requerir una evaluación de riesgos para determinar si los artículos se deberían destruir físicamente en lugar de enviar a reparar o desechar. La información se puede ver comprometida por eliminación o reutilización descuidada de los equipos.

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 suficientemente fuerte y cubre todo el disco (incluyendo el espacio libre y los archivos de intercambio);

b) las claves criptográficas son lo suficientemente largas como para resistir los ataques de fuerza bruta;

c) las propias claves criptográficas se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para más consejos sobre criptografía, ver 8.24.

Las técnicas para sobrescribir de forma segura los medios de almacenamiento difieren según la tecnología de medios de almacenamiento y nivel de clasificación de información en medios de almacenamiento. Las herramientas de sobreescritura se deberían revisar para asegurar que se aplican a la tecnología del medio de almacenamiento.

Ver norma ISO/IEC 27040 para obtener detalles sobre métodos de desinfección de medios de almacenamiento.

8 Controles tecnológicos

8.1 Dispositivos terminales de usuario

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

La información almacenada, procesada o accesible a través de los dispositivos de los usuarios debería estar protegida.

Propósito

Proteger información contra riesgos introducidos por uso de dispositivos terminales del usuario.

Guía

Generalidades

La organización debería establecer una política específica sobre configuración y manejo seguros de dispositivos terminales de usuarios. La política específica del tema se debería comunicar a todo el personal relevante y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos terminales del usuario pueden manejar, procesar, almacenar o soportar;

b) registro de los dispositivos de los usuarios;

c) requisitos de protección física;

d) restricción de la instalación de "software" (por ejemplo, controlada a distancia por los administradores de sistema);

e) requisitos para el software del dispositivo terminales del usuario (incluyendo las versiones del software) y para aplicar las actualizaciones (por ejemplo, la actualización automática activa);

f) normas de conexión a servicios de información, a redes públicas o a cualquier otra red fuera de instalaciones (por ejemplo, exigiendo el uso de un cortafuegos personal);

g) controles de acceso;

h) encriptación del dispositivo de almacenamiento;

i) protección contra "malware";

j) desactivación, borrado o bloqueo a distancia;

k) copias de seguridad;

l) uso de servicios y aplicaciones Web;

m) análisis de comportamiento del usuario final (ver 8.16);

n) uso de dispositivos extraíbles, incluyendo dispositivos de memoria extraíbles y posibilidad de desactivar puertos físicos (por ejemplo, puertos USB);

o) el uso de capacidades de partición, si el dispositivo terminal de usuario admite, que puede separar de forma segura la información de la organización y otros activos asociados (por ejemplo, el "software") de otra información y otros activos asociados en el dispositivo.

Se debería considerar si cierta información es tan sensible que solo se puede acceder a ella a través de dispositivos de usuarios, pero no se puede almacenar en dichos dispositivos. En tales casos, se pueden exigir salvaguardias técnicas adicionales en el dispositivo. Por ejemplo, asegurar que la descarga de archivos para trabajar sin conexión está desactivada y que el almacenamiento local, como la tarjeta SD, está desactivado.

En la medida de lo posible, las recomendaciones sobre este control se deberían aplicar a través de gestión de configuración (ver 8.9) o de herramientas automatizadas.

Responsabilidad de usuario

Todos los usuarios deberían conocer los requisitos y procedimientos de seguridad para la protección de dispositivos de los usuarios, así como sus responsabilidades en la aplicación de dichas medidas de seguridad. Se debería aconsejar a los usuarios que:

a) cerrar las sesiones activas y terminar los servicios cuando ya no sean necesarios;

b) proteger dispositivos terminales de los usuarios del uso no autorizado con un control físico (por ejemplo, bloqueo con llave o cerraduras especiales) y un control lógico (por ejemplo, acceso con contraseña) cuando no se utilicen; no dejar desatendidos dispositivos que transportan información importante, sensible o crítica para la empresa;

c) usar dispositivos con especial atención en lugares públicos, oficinas abiertas, lugares de reunión y otras zonas no protegidas (por ejemplo, evitar la lectura de información confidencial si la gente puede leer por detrás, usar filtros de pantalla de privacidad);

d) proteger físicamente dispositivos terminales de usuarios contra robo (por ejemplo, en autos y otros medios de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Se debería establecer un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales (incluyendo los seguros) y otros requisitos de seguridad de la organización para los casos de robo o pérdida de dispositivos terminales de los usuarios.

Uso de dispositivos personales

Cuando la organización permita el uso de dispositivos personales (a veces conocido como 'BYOD'), además de orientaciones dadas en este control, se debería considerar lo siguiente:

a) separación del uso personal y profesional de dispositivos, incluyendo el uso de software para apoyar dicha separación y proteger los datos profesionales en un dispositivo privado;

b) proporción acceso a información de empresa solo después que los usuarios hayan reconocido sus obligaciones (protección física, actualización de "software", otro), renunciando a la propiedad de datos de la empresa, permitiendo el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no se esté autorizado a usar el servicio. En estos casos, se debería tener en cuenta la legislación de protección de la información personal;

c) evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada políticas y procedimientos específicos del tema;

d) acceder a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que puede ser impedido por la legislación;

e) acordar licencia de "software" son tales que las organizaciones pueden llegar a ser responsables de la concesión de licencias para el "software" del cliente en dispositivos terminales del usuario que son propiedad privada del personal o de usuarios externos.

Conexiones inalámbricas

La organización debería establecer procedimientos para:

a) la configuración de las conexiones inalámbricas en los dispositivos (por ejemplo, desactivando los protocolos vulnerables);

b) la utilización de conexiones inalámbricas o por cable con un ancho de banda adecuado de acuerdo con políticas específicas del tema (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de "software").

Otra información

Los controles para proteger información en dispositivos terminales del usuario dependen de si el dispositivo terminal del usuario se usa solo dentro de instalaciones y conexiones de red seguras de la organización, o si está expuesto a mayores amenazas físicas y relacionadas con la red fuera de la organización.

Las conexiones inalámbricas para dispositivos terminales del usuario son similares a otros tipos de conexiones de red, pero tienen diferencias importantes que se deberían tener en cuenta a la hora de identificar los controles. En particular, la copia de seguridad de información almacenada en dispositivos terminales de usuario puede fallar a veces debido al limitado ancho de banda de red o porque dispositivos terminales del usuario no están conectados en los momentos en que se programan las copias de seguridad.

En caso de algunos puertos USB, como USB-C, no es posible desactivar el puerto USB porque se usa para otros fines (por ejemplo, entrega de energía y salida de pantalla).

8.2 Derechos de acceso privilegiado

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

La asignación y uso de derechos de acceso privilegiados se deberían restringir y gestionar.

Propósito

Para garantizar que solo usuarios autorizados, componentes de “software” y servicios tengan derechos de acceso privilegiados.

Guía

La asignación de derechos de acceso privilegiados se debería controlar a través de un proceso de autorización de acuerdo con la política específica del tema correspondiente sobre control de acceso (ver 5.15). Se debería tener en cuenta lo siguiente:

a) identificar a usuarios que necesitan derechos de acceso privilegiados para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones);

b) asignar derechos de acceso privilegiados a los usuarios según sea necesario y en función de cada evento, de acuerdo con la política específica de control de acceso (ver 5.15) (por ejemplo, solo a personas con competencia necesaria para llevar a cabo actividades que requieren un acceso privilegiado y sobre base de requisitos mínimos para sus roles funcionales);

c) mantener un proceso de autorización (por ejemplo, determinar quién puede aprobar derechos de acceso privilegiados o no concederlos hasta que el proceso de autorización esté completo) y un registro de todos los privilegios asignados;

d) definir y aplicar requisitos para expiración de derechos de acceso privilegiados;

e) tomar medidas para garantizar que usuarios sean conscientes de sus derechos de acceso privilegiado y de cuándo están en este modo. Posibles medidas incluyen uso de identidades de usuario específicas, configuración de interfaz de usuario o incluso equipos específicos;

f) realizar trabajos con derechos de acceso privilegiados antes puede ser necesaria una nueva autenticación o un paso de autenticación. Requisitos de autenticación para los derechos de acceso privilegiados pueden ser más altos que los requisitos para los derechos de acceso normales;

g) revisar periódicamente y después de cualquier cambio organizativo, a los usuarios que trabajan con derechos de acceso privilegiados para verificar si sus funciones, roles, responsabilidades y competencias siguen calificando para trabajar con derechos de acceso privilegiados (ver 5.18);

h) establecer reglas específicas para evitar el uso de identidades genéricas de usuario de administración (como “root”), en función de las capacidades de configuración de los sistemas. Gestionar y proteger información de autenticación de dichas identidades (ver 5.17);

i) conceder un acceso privilegiado temporal solo durante el tiempo necesario para implementar cambios o actividades aprobadas (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de conceder permanentemente derechos de acceso privilegiado. Esto se suele denominar procedimiento “break glass” y a menudo se automatiza mediante tecnologías de gestión de accesos privilegiados;

j) registrar todos los accesos privilegiados a sistemas con fines de auditoría;

k) no compartir o vincular identidades con derechos de acceso privilegiados a múltiples personas, asignando a cada persona una identidad independiente que permita asignar derechos de acceso privilegiados específicos. Las identidades se pueden agrupar (por ejemplo, definiendo un grupo de administradores) para simplificar la gestión de derechos de acceso privilegiados;

l) usar únicamente identidades con derechos de acceso privilegiados para llevar a cabo tareas administrativas y no para tareas generales del día a día [por ejemplo, consultar el correo electrónico, acceder a la Web (usuarios deberían 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 comunes no pueden realizar. Generalmente los roles de administrador del sistema requieren derechos de acceso privilegiado.

El uso inadecuado de privilegios de administrador de sistema (cualquier característica o facilidad de un sistema de información que permita al usuario anular controles de sistema o de aplicación) es un factor que contribuye en gran medida a fallos o violaciones de sistemas.

En la norma ISO/IEC 29146 se puede encontrar más información relacionada con gestión de acceso y gestión segura de acceso a información y a recursos de tecnologías de información y comunicaciones.

8.3 Restricción de acceso a la información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

El acceso a información y a otros activos asociados debería estar restringido de acuerdo con la política específica de control de acceso establecida.

Propósito

Garantizar solo el acceso autorizado y evitar acceso no autorizado a información y otros activos asociados.

Guía

El acceso a información y a otros activos asociados debería estar restringido de acuerdo con políticas específicas del tema establecido. Para respaldar los requisitos de restricción de acceso, se debería tener en cuenta lo siguiente:

a) no permitir acceso a información sensible por parte de identidades de usuario desconocidas o anónimas. Acceso público o anónimo solo se debería conceder a los lugares de almacenamiento que no contengan información sensible;

b) proporcionar mecanismos de configuración para controlar acceso a información en sistemas, aplicaciones y servicios;

c) controlar datos a los que puede acceder un determinado usuario;

d) controlar qué identidades o grupos de identidades tienen qué acceso, como lectura, escritura, eliminación y ejecución;

e) proporcionar controles de acceso físicos o lógicos para aislamiento de aplicaciones, datos de aplicaciones o sistemas sensibles.

Además, técnicas y procesos de gestión de acceso dinámico para proteger información sensible que tiene un alto valor para la organización se deberían considerar cuando la organización:

a) necesita un control granular sobre quién puede acceder a dicha información, durante qué período y de qué manera;

b) desea compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella;

c) desea gestionar dinámicamente, en tiempo real, uso y distribución de dicha información;

d) desea proteger dicha información contra cambios, copias y distribución no autorizados (incluida la impresión);

e) desea controlar el uso de información;

f) desea dejar constancia de cualquier cambio que se produzca en dicha información en caso de que se requiera una futura investigación.

Las técnicas de gestión dinámica del acceso deberían proteger información a lo largo de todo su ciclo de vida (por ejemplo, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer normas sobre la gestión del acceso dinámico en función de casos de uso específicos considerando:

   6) conceder permisos de acceso en función de la identidad, el dispositivo, la ubicación o la aplicación;

   7) aprovechar esquema de clasificación para determinar qué información necesita proteger con técnicas de gestión dinámica del acceso;

b) establecer procesos operativos, de control y de información, así como la infraestructura técnica de apoyo.

Los sistemas de gestión de acceso dinámico deberían proteger la información al:

a) requerir autenticación, credenciales adecuadas o un certificado para acceder a la información;

b) restringir acceso, por ejemplo, a un plazo determinado (por ejemplo, después de una fecha determinada o hasta una fecha concreta);

c) usar cifrado para proteger información;

d) definir permisos de impresión de información;

e) registrar quién accede a información y cómo se usa;

f) lanzar alertas si se detectan intentos de uso indebido de información.

Otra información

Las técnicas de gestión de acceso dinámico y otras tecnologías de protección de información dinámicas pueden apoyar la protección de información incluso cuando los datos se comparten más allá de la organización de origen, en que no se pueden aplicar controles de acceso tradicionales. 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 un nivel granular y adaptar a lo largo del ciclo de vida de la información.

Las técnicas de gestión de acceso dinámico no sustituyen a la gestión de acceso clásica [por ejemplo, mediante listas de control de acceso (ACLs)], pero pueden añadir más factores de condicionalidad, evaluación en tiempo real, reducción de datos justo a tiempo y otras mejoras que pueden ser útiles para la información más sensible. Ofrecer una forma de controlar acceso fuera del entorno de la organización. Las respuestas a incidentes se pueden apoyar en técnicas de gestión dinámica de acceso, ya que los permisos se pueden modificar o revocar en cualquier momento.

En la norma ISO/IEC 29146 se ofrece información adicional sobre un marco para gestión de accesos.

8.4 Acceso a código fuente

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management #Application_security #Secure_configuration	#Protection

Control

El acceso de lectura y escritura a código fuente, a herramientas de desarrollo y a bibliotecas de "software" se debería gestionar adecuadamente.

Propósito

Para impedir introducción de funciones no autorizadas, evitar cambios involuntarios o malintencionados y mantener confidencialidad de la valiosa propiedad intelectual.

Guía

El acceso a código fuente y a elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y a herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas y entornos de prueba) estrictamente debería estar controlado.

En caso del código fuente, esto se puede lograr controlando el almacenamiento central de dicho código, preferiblemente en un sistema de gestión de código fuente.

El acceso de lectura y de escritura a código fuente puede diferir en función de la función del personal. Por ejemplo, el acceso de lectura a código fuente se puede proporcionar ampliamente dentro de la organización, pero el acceso de escritura a código fuente solo se pone a disposición del personal privilegiado o de propietarios designados. En que los componentes de código se usan por varios desarrolladores dentro de una organización, se debería implementar acceso de lectura a un repositorio de código centralizado. Además, si se usa código abierto o componentes de código de terceros dentro de una organización, acceso de lectura a dichos repositorios de código externos se puede proporcionar ampliamente. Sin embargo, acceso de escritura debería seguir siendo restringido.

Para controlar acceso a bibliotecas de código fuente de programas, se deberían tener en cuenta las siguientes directrices, con el fin de reducir las posibilidades de corrupción de programas informáticos:

a) gestionar acceso a código fuente de programas y a bibliotecas de origen de programas de acuerdo con procedimientos establecidos;

b) conceder acceso de lectura y escritura a código fuente en función de las necesidades de empresa y gestionado para hacer frente a los riesgos de alteración o uso indebido y de acuerdo con procedimientos establecidos;

c) actualizar código fuente y de elementos asociados y concesión de acceso a código fuente de acuerdo con procedimientos de control de cambios (ver 8.32) y solo realizándolo después de haber recibido la autorización correspondiente;

d) no conceder a desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollo que controlen las actividades y autorizaciones sobre el código fuente;

e) mantener listados de programas en un entorno seguro, en qué acceso de lectura y escritura se debería gestionar y asignar adecuadamente;

f) mantener un registro de auditoría de todos accesos y de todos los cambios en el código fuente.

Si se pretende publicar el código fuente del programa, se deberían considerar controles adicionales para garantizar su integridad (por ejemplo, firma digital).

Otra información

Si se accede al código fuente no se controla adecuadamente, este se puede modificar o algunos datos del entorno de desarrollo (por ejemplo, copias de datos de producción, detalles de configuración) se pueden recuperar por personas no autorizadas.

8.5 Autenticación segura

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Las tecnologías y procedimientos de autenticación segura se deberían aplicar en función de las restricciones de acceso a información y de política específica de control de acceso.

Propósito

Garantizar que un usuario o una entidad se autentiquen de forma segura, cuando se conceda acceso a sistemas, aplicaciones y servicios.

Guía

Se debería elegir una técnica de autenticación adecuada para corroborar la identidad reivindicada de un usuario, de “software”, de mensajes y de otras entidades.

La fuerza de autenticación se debería convenir para la clasificación de información a la que se va a acceder. En que se requiera una autenticación fuerte y verificación de identidad, los métodos de autenticación se deberían usar una alternativa a las contraseñas, como certificados digitales, tarjetas inteligentes, “tokens” o medios biométricos.

La información de autenticación debería ir acompañada de factores de autenticación adicionales para acceder a sistemas de información críticos (también conocida como autenticación multifactor). Uso de una combinación de múltiples factores de autenticación, como lo que se sabe, lo que se tiene y que se es, reduce las posibilidades de accesos no autorizados. La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, basadas en reglas y patrones predefinidos, como acceso desde un lugar inusual, dispositivo inusual o en un momento inusual.

La información de autentificación biométrica se debería invalidar si alguna vez se ve comprometida. Autenticación biométrica puede no estar disponible dependiendo de las condiciones de uso (por ejemplo, humedad o envejecimiento). Para estar preparado para estos problemas, la autenticación biométrica debería ir acompañada de al menos una técnica de autenticación alternativa.

El procedimiento de inicio de sesión en un sistema o aplicación debería estar diseñado para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión se deberían implementar teniendo en cuenta lo siguiente:

a) no mostrar información sensible de sistema o de aplicación hasta que el proceso de inicio de sesión se complete con éxito para evitar proporcionar a un usuario no autorizado cualquier ayuda innecesaria;

b) mostrar un aviso general que advierta que el sistema, aplicación o servicio se debería acceder únicamente por usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que puedan ayudar a un usuario no autorizado (por ejemplo, si se produce una condición de error, sistema debería no indicar qué parte de datos es correcta o incorrecta);

d) validar información de inicio de sesión solo cuando se completen todos los datos introducidos;

e) proteger contra los intentos de acceso por fuerza bruta a los nombres de usuario y contraseñas [por ejemplo, usando una prueba de Turing pública completamente automatizada para distinguir a los ordenadores de los humanos (CAPTCHA), exigiendo el restablecimiento de la contraseña tras un número predefinido de intentos fallidos o bloqueando al usuario tras un número máximo de errores];

f) registrar intentos fallidos y exitosos;

g) lanzar un evento de seguridad si se detecta un posible intento o éxito de violación de los controles de inicio de sesión (por ejemplo, enviando una alerta al usuario y a administradores de sistema de la organización cuando se alcanzó un determinado número de intentos de contraseña errónea);

h) mostrar o enviar la siguiente información en un canal separado al finalizar un inicio de sesión exitoso:

   1) fechar y anotar la hora del último inicio de sesión con éxito;

   2) detallar los intentos fallidos de inicio de sesión desde el último inicio de sesión con éxito;

i) no mostrar una contraseña en texto claro cuando se está introduciendo; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión de usuario (por ejemplo, por razones de accesibilidad o para evitar bloqueo de usuarios debido a errores repetidos);

j) no transmitir contraseñas en texto claro a través de la red para evitar que se capten por un programa “sniffer[7]” de la red;

7 Del inglés sniffer: *husmeador, oledor o sabueso.*

k) terminar sesiones inactivas después de un período definido de inactividad, especialmente en lugares de alto riesgo como áreas públicas o externas fuera de gestión de seguridad de la organización o en dispositivos de usuarios;

l) restringir tiempos de duración de conexión para proporcionar seguridad adicional a aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Otra información

En la norma ISO/IEC 29115 se puede encontrar información adicional sobre la garantía de autenticación de entidades.

8.6 Gestión de capacidad

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_ Ecosystem #Protection

Control

El uso de recursos se debería supervisar y ajustar en función de necesidades y capacidad actuales y previstas.

Propósito

Garantizar capacidad necesaria de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

Guía

Se deberían identificar necesidades de capacidad de instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones, teniendo en cuenta la criticidad de sistemas y procesos en cuestión.

El ajuste y supervisión de sistema se deberían aplicar para garantizar y, en que sea necesario, mejorar la disponibilidad y eficiencia de sistemas.

La organización debería realizar pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad de sistema para cumplir con los requisitos de rendimiento máximo.

Se deberían establecer controles de detección para indicar los problemas a su debido tiempo.

Las proyecciones de futuras necesidades de capacidad deberían tener en cuenta las nuevas necesidades de la empresa y de sistema, así como las tendencias actuales y previstas de capacidades de procesamiento de información de la organización.

Se debería prestar especial atención a los recursos con largos plazos de adquisición o costes elevados. Por lo tanto, los gestores, propietarios de servicios o productos deberían supervisar la utilización de recursos clave de sistema.

Los gestores deberían usar información sobre la capacidad para identificar y evitar las posibles limitaciones de recursos y dependencia del personal clave que puedan suponer una amenaza para la seguridad de sistema o los servicios y planificar las medidas adecuadas.

Se puede conseguir una capacidad suficiente aumentando la capacidad o reduciendo la demanda. Para aumentarla hay que tener en cuenta lo siguiente:

a) contratar nuevo personal;

b) obtener nuevas instalaciones o espacios;

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 problemas de capacidad. La computación en la nube tiene elasticidad, escalabilidad que permiten ampliar, reducir rápidamente recursos disponibles para determinadas aplicaciones y servicios

Para reducir la demanda de recursos de la organización, se debería considerar lo siguiente:

a) eliminar datos obsoletos (espacio en disco);

b) eliminar de documentos impresos que han cumplido su período de conservación (para liberar espacio en estanterías);

c) desmantelar aplicaciones, sistemas, bases de datos o entornos;

d) optimizar procesos y programas por lotes;

e) optimizar código de la aplicación o consultas a la base de datos;

f) negar o restringir el ancho de banda de servicios que consumen recursos si no son críticos (por ejemplo, transmisión de vídeo).

Se debería considerar un plan de gestión de la capacidad documentado para los sistemas de misión crítica.

Otros datos

Para más detalles sobre elasticidad y escalabilidad de la computación en la nube, ver norma ISO/IEC TS 23167.

8.7 Protección contra “malware”

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_ security #Information_ protection	#Protection #Defence

Control

La protección contra el “malware” se debería implementar y respaldar mediante la conciencia adecuada del usuario.

Propósito

Garantizar protección de información y otros activos asociados contra “malware”.

Guía

La protección contra el “malware” se debería basar en el “software” de detección y reparación de “malware”, en la concientización sobre seguridad de información, en el acceso adecuado al sistema y en controles de gestión de cambios. Uso de “software” de detección y reparación de “malware” por sí solo no suele ser conveniente. Se deberían tener en cuenta las orientaciones siguientes:

a) implementar reglas y controles que impidan o detecten el uso de “software” no autorizado [por ejemplo, el uso de una lista de aplicaciones permitidas] (ver 8.19 y 8.32);

b) aplicar controles que impidan o detecten el uso de sitios Web conocidos o sospechosos de ser maliciosos (por ejemplo, listas de bloqueo);

c) reducir vulnerabilidades que se pueden explotar por el “malware” [por ejemplo, mediante gestión técnica de vulnerabilidades (ver 8.8 y 8.19)];

d) realizar una validación periódica y automatizada de contenido de “software” y de datos de sistemas, especialmente en el caso de sistemas que soportan procesos empresariales críticos; investigar la presencia de cualquier archivo no aprobado o de modificaciones no autorizadas;

e) establecer medidas de protección contra riesgos asociados a obtención de archivos y programas informáticos desde o a través de redes externas o en cualquier otro soporte;

f) instalar y actualizar periódicamente “malware” de detección, reparación para escanear computadores y medios de almacenamiento electrónico. Llevar a cabo escaneos regulares que incluyan:

   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 usarlos. Realizar este escaneo en diferentes lugares (por ejemplo, en servidores de correo electrónico, computadores de sobremesa) y al entrar en red de la organización;

   3) escanear páginas Web en busca de “malware” cuando se accede a ellas;

g) determinar ubicación y configuración de herramientas de detección y reparación de “malware” en función de resultados de evaluación de riesgos y considerando:

   1) principios de defensa en profundidad en que sean más eficaces. Por ejemplo, esto puede llevar a la detección de “malware” en una pasarela de red (en varios protocolos de aplicación como el correo electrónico, la transferencia de archivos y la Web), así como en los dispositivos y servidores de los usuarios;

2) las técnicas evasivas de los atacantes (por ejemplo, el uso de archivos cifrados) para entregar "malware" o el uso de protocolos de cifrado para transmitir "malware";

h) poner especial atención en la protección contra la introducción de "malware" durante procedimientos de mantenimiento y emergencia, que pueden eludir 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", incluyendo autoridades de aprobación de excepciones, justificación documentada y fecha de revisión. Esto puede ser necesario cuando la protección contra el "malware" causa interrupción de operaciones normales;

j) preparar planes adecuados de continuidad de actividad para recuperarse de ataques de "malware", incluyendo todas las copias de seguridad de datos y "software" necesarias (incluyendo las copias de seguridad en línea y fuera de línea) y medidas de recuperación (ver 8.13);

k) aislar entornos en que se pueden producir consecuencias catastróficas;

l) definir procedimientos y responsabilidades para tratar la protección contra el "malware" en sistemas, incluyendo formación en su uso, notificación y recuperación de ataques de "malware";

m) proporcionar concientización o formación (ver 6.3) a todos los usuarios sobre cómo identificar y potencialmente mitigar la recepción, envío o instalación de correos electrónicos, archivos o programas infectados con "malware" [información recogida en n) y o) se puede usar para garantizar que la concientización y formación se mantienen actualizadas];

n) aplicar procedimientos para recopilar periódicamente información sobre nuevo "malware", como la suscripción a listas de correo o la revisión de sitios Web relevantes;

o) verificar que la información relativa al "malware", como boletines de advertencia, procede de fuentes cualificadas y acreditadas (por ejemplo, sitios de Internet fiables o proveedores de "software" de detección de "malware") y es precisa e informativa.

Otra información

No siempre es posible instalar "software" que proteja contra el "malware" en algunos sistemas (por ejemplo, algunos sistemas de control industrial). Algunas formas de "malware" infectan los sistemas operativos y el firmware de los computadores de tal manera que los controles comunes de "malware" no pueden limpiar el sistema y es necesario imaginar de nuevo y por completo el "software" de sistema operativo y a veces, "firmware" del computador para volver a un estado seguro.

8.8 Gestión de vulnerabilidades técnicas

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_and_ Ecosystem #Protection #Defence

Control

Se debería obtener información sobre vulnerabilidades técnicas de sistemas de información en uso, evaluar exposición de la organización a dichas vulnerabilidades y tomar medidas adecuadas.

Propósito

Para evitar la explotación de las vulnerabilidades técnicas.

Guía

Identificación de vulnerabilidades técnicas

La organización debería contar con un inventario preciso de activos (ver 5.9 a 5.14) como requisito previo para una gestión eficaz de vulnerabilidad técnica; el inventario debería incluir el proveedor de “software”, el nombre de “software”, los números de versión, el estado actual de despliegue (por ejemplo, qué “software” está instalado en qué sistemas) y la persona o personas dentro de la organización responsables de “software”.

Para identificar las vulnerabilidades técnicas, la organización debería considerar:

a) definir y establecer funciones y responsabilidades asociadas a la gestión técnica de vulnerabilidad, incluida supervisión de vulnerabilidad, evaluación de riesgo de esta, actualización, monitoreo de activos y cualquier responsabilidad de coordinación necesaria;

b) identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento de las mismas, en el caso de programas informáticos y otras tecnologías (sobre la base de la lista de inventario de activos, (ver 5.9). Actualizar la lista de recursos de información en función de cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles;

c) exigir a proveedores de sistemas de información (incluyendo sus componentes) que garanticen la notificación, tratamiento y divulgación de vulnerabilidad, incluyendo requisitos de contratos aplicables (ver 5.20);

d) usar herramientas de exploración de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si la aplicación de parches a las vulnerabilidades fue exitosa;

e) realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Tener precaución, ya que estas actividades pueden llevar a comprometer la seguridad de sistema;

f) rastrear uso de bibliotecas y código fuente de terceros en busca de vulnerabilidades. Esto se debería incluir en la codificación segura (ver 8.28).

La organización debería desarrollar procedimientos y capacidades para:

a) detectar existencia de vulnerabilidades en sus productos y servicios, incluyendo cualquier componente externo usado en ellos;

b) recibir informes de vulnerabilidad de fuentes internas o externas.

La organización debería proporcionar un punto de contacto público como parte de una política específica sobre divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar de los problemas. La organización debería establecer procedimientos de notificación de vulnerabilidades, formularios de notificación en línea y hacer uso de los foros adecuados de inteligencia de amenazas o de intercambio de información. La organización también debería considerar programas de recompensas por errores en que se ofrezcan recompensas como incentivo para ayudar a las organizaciones a identificar las vulnerabilidades con el fin de remediarlas adecuadamente. La organización también debería compartir información con los organismos competentes del sector u otras partes interesadas.

Evaluación de vulnerabilidades técnicas

Para evaluar vulnerabilidades técnicas identificadas, se deberían tener en cuenta las siguientes orientaciones:

a) analizar y verificar los informes para determinar qué actividad de respuesta y reparación es necesaria;

b) identificar los riesgos asociados y las acciones a realizar, una vez identificada una posible vulnerabilidad técnica. Estas acciones pueden consistir en la actualización de los sistemas vulnerables o en la aplicación de otros controles.

Medidas apropiadas para hacer frente a las vulnerabilidades técnicas

Se debería implantar un proceso de gestión de actualizaciones de “software” para garantizar que se instalan los parches y actualizaciones de aplicaciones más recientes para todo el “software” autorizado. Si es necesario realizar cambios, se debería conservar el “software” original y aplicar los cambios a una copia designada. Todos los cambios se deberían probar y documentar por completo, de modo que se puedan volver a aplicar, si es necesario, a futuras actualizaciones de “software”. Si es necesario, las modificaciones se deberían aprobar y validar por un organismo de evaluación independiente.

Las siguientes orientaciones se deberían considerar para abordar vulnerabilidades técnicas:

a) tomar medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un calendario para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

b) llevar a cabo la acción según los controles relacionados con la gestión del cambio (ver 8.32) o siguiendo procedimientos de respuesta a incidentes de seguridad de información (ver 5.26), dependiendo de la urgencia con la que haya que abordar una vulnerabilidad técnica;

c) usar actualizaciones de fuentes legítimas únicamente (que pueden ser internas o externas a la organización);

d) probar y evaluar actualizaciones antes de instalarlas para garantizar que son eficaces y no provocan efectos secundarios que no se puedan tolerar [por ejemplo, si hay una actualización disponible, evaluar los riesgos asociados a la instalación de la actualización (riesgos que plantea la vulnerabilidad se deberían comparar con riesgo de instalar la actualización)];

e) abordar primero sistemas de alto riesgo;

f) desarrollar soluciones (normalmente actualizaciones o parches de “software”);

g) prueba para confirmar si la corrección o mitigación es eficaz;

h) proporcionar mecanismos para verificar autenticidad de la reparación;

i) tener en cuenta otros controles, como, si no hay ninguna actualización disponible o esta no se puede instalar:

   1) aplicar cualquier solución sugerida por el proveedor de “software” u otras fuentes relevantes;

   2) desactivar servicios o capacidades relacionados con vulnerabilidad;

   3) adaptar o añadir controles de acceso (por ejemplo, cortafuegos) en las fronteras de red (ver 8.20 a 8.22);

   4) blindar sistemas, dispositivos o aplicaciones vulnerables contra ataques mediante despliegue de filtros de tráfico adecuados (a veces llamados parches virtuales);

   5) aumentar vigilancia para detectar ataques reales;

   6) sensibilizar sobre vulnerabilidad.

En el caso de “software” adquirido, si los proveedores publican regularmente información sobre actualizaciones de seguridad de su “software” y proporcionan una facilidad para instalar dichas actualizaciones automáticamente, la organización debería decidir si usar actualización automática o no.

Otras consideraciones

Se debería mantener un registro de auditoría para todos los pasos realizados en gestión de vulnerabilidad técnica.

El proceso de gestión de vulnerabilidad técnica se debería supervisar, evaluar periódicamente para garantizar su eficacia y eficiencia.

Un proceso eficaz de gestión de vulnerabilidad técnica debería 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 deberían llevar a cabo en caso de que se produzca un incidente.

Cuando la organización usa un servicio en la nube suministrado por un proveedor de servicios en la nube de terceros, la gestión de vulnerabilidad técnica de los recursos del proveedor de servicios en la nube se debería garantizar por el proveedor de servicios en la nube. Las responsabilidades del proveedor de servicios en la nube en cuanto a la gestión de vulnerabilidad técnica deberían formar parte del acuerdo de servicios en la nube y esto debería incluir procesos para informar de las acciones del proveedor de servicios en la nube relacionadas con las vulnerabilidades técnicas (ver 5.23). Para algunos servicios en la nube, existen responsabilidades respectivas para el proveedor de servicios en la nube y el cliente de servicios en la nube. Por ejemplo, el cliente de servicios en la nube es responsable de gestión de vulnerabilidad de sus propios activos usados para servicios en la nube.

Otra información

La gestión de vulnerabilidad técnica se puede considerar como una subfunción de gestión de cambio y, como tal, puede aprovechar procesos y procedimientos de gestión de cambio (ver 8.32).

Existe la posibilidad de que una actualización no resuelva el problema adecuadamente y tenga efectos secundarios negativos. Además, en algunos casos, no es fácil desinstalar una actualización una vez que se aplicó.

Si no es posible realizar pruebas adecuadas de actualizaciones (por ejemplo, debido a los costes o a la falta de recursos), se puede considerar un retraso en actualización para evaluar los riesgos asociados, basándose en la experiencia de otros usuarios. El uso de la norma ISO/IEC 27031 puede ser beneficioso.

Cuando se produzcan parches o actualizaciones de “software”, la organización puede considerar la posibilidad de ofrecer un proceso de actualización automatizado en que estas actualizaciones se instalen en los sistemas o productos afectados sin necesidad de que intervenga el cliente o el usuario. Si se ofrece un proceso de actualización automatizado, puede permitir al cliente o al usuario elegir una opción para desactivar actualización automática o controlar el momento de la instalación de actualización.

Cuando el proveedor proporciona un proceso de actualización automatizado y 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 de las razones para no elegir actualización automatizada es mantener el control sobre cuándo se realiza actualización. Por ejemplo, un “software” usado para una operación comercial no se puede actualizar hasta que la operación finalice.

Un punto débil del escáner de vulnerabilidad es que es posible que no tenga en cuenta totalmente defensa en profundidad: dos contramedidas que se invocan siempre en secuencia pueden tener vulnerabilidades que se enmascaran por los puntos fuertes de la otra. La contramedida compuesta no es vulnerable, mientras que un escáner de vulnerabilidad puede informar de que ambos componentes son vulnerables. Por lo tanto, la organización debería poner especial atención 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 afectan a la seguridad de los usuarios.

Las organizaciones pueden publicar la corrección y divulgar información sobre vulnerabilidades a usuarios (normalmente a través de un aviso público) y proporcionar información adecuada para servicios de la base de datos de vulnerabilidades de “software”.

Para más información relacionada con la gestión de vulnerabilidades técnicas cuando se usa la computación en la nube, ver las normas ISO/IEC 19086 e ISO/IEC 27017.

La norma ISO/IEC 29147 proporciona información detallada sobre la recepción de informes de vulnerabilidad y publicación de avisos de vulnerabilidad. La norma ISO/IEC 30111 proporciona información detallada sobre gestión y resolución de vulnerabilidades notificadas.

8.9 Gestión de configuración

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

Las configuraciones, incluyendo las configuraciones de seguridad, de “hardware”, “software”, servicios y redes se deberían establecer, documentar, aplicar, supervisar y revisar.

Propósito

Garantizar que “hardware”, “software”, servicios y redes funcionen correctamente con ajustes de seguridad requeridos y que la configuración no se vea alterada por cambios no autorizados o incorrectos.

Guía

Generalidades

La organización debería definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluyendo las configuraciones de seguridad) para el “hardware”, “software”, servicios (por ejemplo, los servicios en la nube) y las redes, tanto para los sistemas recién instalados como para sistemas operativos durante su vida útil.

Se deberían establecer funciones, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración.

Plantillas estándar

Se deberían definir plantillas estándar para la configuración segura de “hardware”, “software”, servicios y redes:

a) usar orientaciones disponibles públicamente (por ejemplo, plantillas predefinidas de los proveedores y de organizaciones de seguridad independientes);

b) considerar nivel de protección necesario para determinar un nivel de seguridad suficiente;

c) apoyar política de seguridad de información de la organización, políticas específicas del tema, normas y otros requisitos de seguridad;

d) considerar viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas se deberían revisar periódicamente y actualizar cuando haya que hacer frente a nuevas amenazas, vulnerabilidades o cuando se introduzcan nuevas versiones de “software” o “hardware”.

Para el establecimiento de plantillas estándar para la configuración segura de “hardware”, “software”, servicios y redes se debería considerar lo siguiente:

a) minimizar número de identidades con derechos de acceso de nivel privilegiado o de administrador;

b) desactivar identidades innecesarias, no usadas o inseguras;

c) desactivar o restringir funciones y servicios innecesarios;

d) restringir acceso a potentes programas de utilidad y a configuración de parámetros del servidor;

e) sincronizar relojes;

f) cambiar información de autenticación por defecto del proveedor, como contraseñas por defecto, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad por defecto;

g) invocar instalaciones de tiempo de espera que desconecten automáticamente dispositivos informáticos después de un período predeterminado de inactividad;

h) verificar el cumplimiento de los requisitos de la licencia (ver 5.32).

Gestión de las configuraciones

Las configuraciones establecidas de “hardware”, “software”, servicios y redes se deberían registrar y se debería mantener un registro de todos los cambios de configuración. Estos registros se deberían almacenar 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 deberían seguir el proceso de gestión de cambios (ver 8.32).

Los registros de configuración pueden contener lo pertinente:

a) información actualizada del propietario o punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de plantilla de configuración;

d) relación con configuraciones de otros activos.

Configuraciones de control

Las configuraciones se deberían monitorear con un conjunto integral de herramientas de administración del sistema (por ejemplo, utilidades de mantenimiento, soporte remoto, herramientas de administración empresarial, software de copia de seguridad y restauración) y se deberían revisar 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 definidas. Cualquier desviación se debería abordar, ya sea mediante la aplicación automática de la configuración objetivo que se define mediante el análisis manual de la desviación seguido de acciones correctivas.

Otra información

La documentación de los sistemas suele registrar detalles sobre configuración tanto de “hardware” como de “software”.

El endurecimiento de sistema es una parte típica de gestión de configuración.

La gestión de configuración se puede integrar con los procesos de gestión de activos y herramientas asociadas.

La automatización suele ser más eficaz para gestionar la configuración de seguridad (por ejemplo, usando infraestructura como código).

Las plantillas de configuración y objetivos pueden ser información confidencial y se deberían proteger de acceso no autorizado en consecuencia.

8.10 Supresión de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

Control

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debería eliminar cuando ya no sea necesaria.

Propósito

Evitar la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales de eliminación de información.

Guía

Generalidades

La información sensible no se debería conservar durante más tiempo del necesario para reducir el riesgo de divulgación no deseada.

Al momento de eliminar la información de los sistemas, aplicaciones y servicios, se debería tener en cuenta lo siguiente:

a) seleccionar un método de borrado (por ejemplo, sobreescritura electrónica o borrado criptográfico) de acuerdo con los requisitos de la empresa y teniendo en cuenta leyes y reglamentos pertinentes;

b) registrar resultados de eliminación como prueba;

c) obtener pruebas de la eliminación de información de ellos, cuando se usen proveedores de servicios de eliminación de información.

Cuando terceros almacenan información de la organización en su nombre, esta debería considerar la inclusión de requisitos sobre eliminación de la información en los acuerdos con terceros para hacerlos cumplir durante y tras la finalización de dichos servicios.

Métodos de supresión

De acuerdo con la política específica de la organización en materia de conservación de datos y teniendo en cuenta legislación y reglamentos pertinentes, información sensible se debería eliminar cuando ya no sea necesaria, por:

a) configurar sistemas para que destruyan de forma segura información cuando ya no sea necesaria (por ejemplo, después de un periodo definido sujeto a la política específica de conservación de datos o por solicitud de acceso del sujeto);

b) eliminar versiones obsoletas, copias y archivos temporales dondequiera que se encuentren;

c) usar programas informáticos de borrado seguros y aprobados para eliminar permanentemente información, con el fin de garantizar que esta no se pueda recuperar mediante herramientas forenses o de recuperación especializadas;

d) usar proveedores autorizados y certificados de servicios de eliminación segura;

e) usar mecanismos de eliminación adecuados para el tipo de medios de almacenamiento que se eliminan (por ejemplo, desmagnetizando unidades de disco duro y otros medios de almacenamiento magnético).

Cuando se usen servicios en la nube, la organización debería verificar si el método de borrado proporcionado por proveedor de servicios en la nube es aceptable y si es el caso, la organización debería usarlo o solicitar que el proveedor de servicios en la nube borre información. Estos procesos de borrado deberían estar automatizados en acuerdo con políticas específicas del tema, cuando estén disponibles y sean aplicables. Dependiendo de la sensibilidad de información eliminada, registros pueden rastrear o verificar que estos procesos de eliminación han ocurrido.

Para evitar la exposición involuntaria de información sensible cuando los equipos se devuelven a proveedores, la información sensible se debería proteger eliminando los almacenamientos auxiliares (por ejemplo, los discos duros) y memoria antes de que los equipos salgan de las instalaciones de la organización.

Al considerar que el borrado seguro de algunos dispositivos (por ejemplo, teléfonos inteligentes) solo se puede lograr a través de la destrucción o usando funciones incorporadas en estos dispositivos (por ejemplo, “restablecer la configuración de fábrica”), la organización debería elegir el método adecuado en función de clasificación de información manejada por dichos dispositivos.

Las medidas de control descritas en 7.14 se deberían aplicar para destruir físicamente el dispositivo de almacenamiento y simultáneamente, borrar la información que contiene.

Un registro oficial de la eliminación de información es útil a la hora de analizar la causa de un posible evento de fuga de información.

Otra información

La información sobre eliminación de datos de usuarios en servicios en la nube se puede encontrar en la norma ISO/IEC 27017. En la norma ISO/IEC 27555 se puede encontrar información sobre la eliminación de PII.

8.11 Enmascaramiento de datos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

Control

El enmascaramiento de datos se debería usar de acuerdo con la política específica de la organización sobre control de acceso y otras políticas específicas relacionadas con el tema, así como con los requisitos empresariales, teniendo en cuenta la legislación aplicable.

Propósito

Para limitar la exposición de datos sensibles, incluida la información personal, y para cumplir con los requisitos legales, reglamentarios y contractuales.

Guía

Cuando la protección de datos sensibles (por ejemplo, PII) es una preocupación, la organización debería considerar la posibilidad de 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 PII, disimular la verdadera identidad de los titulares de PII u otra información sensible, y desconectar el vínculo entre PII y la identidad del titular de PII o el vínculo entre otra información sensible.

Cuando se usan técnicas de seudonimización o anonimización, se debería verificar que los datos han sido adecuadamente seudonimizados o anonimizados. La anonimización de datos debería considerar todos los elementos de la información sensible para que sea efectiva. Por ejemplo, si no se considera adecuadamente, se puede identificar a una persona, aunque se anonimicen los datos que pueden identificarla directamente, por la presencia de otros datos que permiten identificarla indirectamente.

Otras técnicas de enmascaramiento de datos son:

a) encriptación (que requiere que los usuarios autorizados tengan una clave);

b) anulación o eliminación de 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) sustitución de valores por su almohadilla.

Al momento de aplicar las técnicas de enmascaramiento de datos se debería tener en cuenta lo siguiente:

a) no concesión a todos los usuarios acceso a todos los datos, por lo que se diseñan consultas y máscaras para mostrar solo datos mínimos necesarios al usuario;

b) diseño e implementación un mecanismo de ofuscación de datos, en este caso (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 de hospital se presenta con datos parcialmente ofuscados y datos solo pueden ser accedidos por el personal con roles específicos si contienen información útil para el tratamiento adecuado), hay casos en que algunos datos deberían no ser visibles para el usuario para algunos registros de un conjunto de datos;

c) cuando los datos están ofuscados, dando al mandante 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 centros sanitarios, por ejemplo, si el paciente no quiere que el personal vea que se ofuscó información sensible como embarazos o resultados de exámenes de sangre);

d) cualquier requisito legal o reglamentario (por ejemplo, exigir enmascaramiento de información de tarjetas de pago durante procesamiento o almacenamiento).

Al momento de usar enmascaramiento, seudonimización o anonimización de datos, se debería tener en cuenta lo siguiente:

a) nivelar intensidad de enmascaramiento, seudonimización o anonimización de datos en función de uso de datos tratados;

b) controlar acceso a datos tratados;

c) acordar o restricciones de uso de datos tratados;

d) prohibir cotejar datos procesados con otra información para identificar al titular de la información personal;

e) llevar control de entrega y recepción de datos procesados.

Otra información

La anonimización altera de forma irreversible la PII, de tal manera que el titular de esta ya no puede ser identificado directa o indirectamente.

La seudonimización sustituye la información de identificación por un alias. El Conocimiento de algoritmo (a veces denominado “información adicional”) usado para llevar a cabo la seudonimización permite al menos alguna forma de identificación del principal de PII. Por lo tanto, dicha “información adicional” se debería mantener separada y protegida.

Aunque la seudonimización es, por tanto, más débil que la anonimización, conjuntos de datos seudonimizados pueden ser más útiles en investigación estadística.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos sensibles. El enmascaramiento de datos puede ser estático (cuando los elementos de datos se enmascaran en la base de datos original), dinámico (usando automatización y reglas para asegurar los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Las funciones hash se pueden usar para anonimizar PII. Para evitar ataques de enumeración, se deberían combinar siempre con una función salt.

La PII en identificadores de recursos y sus atributos [por ejemplo, nombres de archivos, localizadores uniformes de recursos (URL)] se debería evitar o anonimizar adecuadamente.

En la norma ISO/IEC 27018 se ofrecen controles adicionales relativos a la protección de PII en las nubes públicas.

En la norma ISO/IEC 20889 se ofrece información adicional sobre las técnicas de desidentificación.

8.12 Prevención fuga de datos

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence

Control

Las medidas de prevención de fuga de datos se deberían aplicar a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

Propósito

Detectar e impedir divulgación y extracción no autorizada de información por parte de personas o sistemas.

Guía

La organización debería considerar lo siguiente para reducir el riesgo de fuga de datos:

a) identificar y clasificar información para protegerla contra las filtraciones (por ejemplo, información personal, modelos de precios y diseños de productos);

b) controlar canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles);

c) actuar para evitar filtración de información (por ejemplo, poner en cuarentena los correos electrónicos que contengan información sensible).

Se deberían utilizar herramientas de prevención de fuga de datos para:

a) identificar y controlar información sensible que corre riesgo de ser revelada sin autorización (por ejemplo, en datos no estructurados de sistema de un usuario);

b) detectar divulgación de información sensible (por ejemplo, cuando la información se sube a servicios en la nube de terceros que no son de confianza o se envía por correo electrónico);

c) bloquear acciones de usuarios o transmisiones de red que expongan información sensible (por ejemplo, impedir la copia de entradas de base de datos en una hoja de cálculo).

La organización debería 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 debería implementar tecnología como herramientas de prevención de fuga de datos o configuración de herramientas existentes que permitan a usuarios ver y manipular datos mantenidos de forma remota pero que impidan copiar y pegar fuera del control de la organización.

Si se requiere exportación de datos, el propietario de datos debería poder aprobar la exportación y hacer que los usuarios sean responsables de sus acciones.

La toma de capturas de pantalla o de fotografías de pantalla se debería abordar a través de los términos y condiciones de uso, formación y auditoría.

Cuando se hace una copia de seguridad de datos, se debería asegurar de que la información sensible está protegida con medidas como el cifrado, control de acceso y protección física de medios de almacenamiento que contienen la copia de seguridad.

La prevención de la fuga de datos también se debería considerar para ser protegido de las acciones de inteligencia de un adversario para obtener información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o cualquier otra) que pueda ser de interés para el espionaje o pueda ser crítica para la comunidad. Las acciones de prevención de la fuga de datos deberían estar orientadas a confundir las decisiones del adversario, por ejemplo, sustituyendo información auténtica por información falsa, ya sea como acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o uso de honeypots[8] para atraer a los atacantes.

Otra información

Las herramientas de prevención de fuga de datos están diseñadas para identificar datos, supervisar su uso, movimiento y tomar medidas para evitar que se filtren (por ejemplo, alertando a usuarios de su comportamiento arriesgado y bloqueando la transferencia de datos a dispositivos de almacenamiento portátiles).

La prevención de fuga de datos implica intrínsecamente la supervisión de comunicaciones y actividades en línea del personal y, por extensión, de mensajes de partes externas, lo que plantea problemas legales que se deberían tener en cuenta antes de desplegar herramientas de prevención de fuga de datos. Existe una variedad de legislación relativa a privacidad, protección de datos, empleo, interceptación de datos y telecomunicaciones que es aplicable a supervisión y tratamiento de datos en el contexto de prevención de fuga de datos.

La prevención de fuga de datos se puede apoyar en controles de seguridad estándar, como políticas específicas de control de acceso y gestión segura de documentos (ver 5.12 y 5.15).

8.13 Respaldo de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Control

Las copias de seguridad de la información, de “software” y de sistemas se deberían mantener y probar periódicamente de acuerdo con la política específica acordada sobre copias de seguridad.

Propósito

Para permitir recuperación de pérdida de datos o sistemas.

8 Del inglés honeypots: *red trampa, sistema trampa o tarro de miel.*

Guía

Se debería establecer una política específica sobre copias de seguridad para abordar los requisitos de retención de datos y seguridad de información de la organización.

Se deberían proporcionar instalaciones de copia de seguridad adecuadas para garantizar que toda información esencial y “software” se pueda recuperar tras un incidente o fallo o pérdida de medios de almacenamiento.

Se deberían desarrollar e implementar planes sobre cómo la organización hará copias de seguridad de información, “software” y sistemas, para abordar la política específica sobre copias de seguridad.

Al momento de diseñar un plan de respaldo, se deberían tener en cuenta los elementos siguientes:

a) elaborar registros precisos y completos de copias de seguridad y de procedimientos de restauración documentados;

b) reflejar los requisitos de negocio de la organización (por ejemplo, el objetivo del punto de recuperación, ver 5.30), requisitos de seguridad de la información implicada y criticidad de información para funcionamiento continuo de la organización en el alcance (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de copias de seguridad;

c) almacenar copias de seguridad en una ubicación remota segura, 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 apropiado de protección física y ambiental (ver cláusula 7 y 8.1) consistente con los estándares aplicados en el sitio principal;

e) probar periódicamente los medios de copia de seguridad para garantizar que se puede confiar en ellos para un uso de emergencia cuando sea necesario. Probar la capacidad de restaurar datos de copias de seguridad en un sistema de prueba, no sobrescribiendo el medio de almacenamiento original en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas de datos irreparables;

f) proteger copias de seguridad mediante cifrado en función de riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad es importante);

g) poner especial atención en que pérdida de datos involuntaria se detecte antes de realizar la copia de seguridad.

Los procedimientos operativos deberían supervisar la ejecución de copias de seguridad y abordar los fallos de copias de seguridad programadas para garantizar la integridad de esta de acuerdo con la política específica sobre copias de seguridad.

Las medidas de copia de seguridad de los sistemas y servicios individuales se deberían probar regularmente para garantizar que cumplen objetivos de planes de respuesta a incidentes y de continuidad del negocio (ver 5.30). Esto se debería combinar con una prueba de procedimientos de restauración y cotejar con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de los sistemas y servicios críticos, medidas de copia de seguridad deberían cubrir toda la información de sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en caso de desastre.

Cuando la organización usa un servicio en la nube, se deberían realizar copias de seguridad de la información, aplicaciones y sistemas de la organización en el entorno del servicio en la nube. La organización debería determinar si se cumplen los requisitos para la realización de copias de seguridad, y cómo, cuándo se usa el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube.

Se debería determinar el período de conservación de información empresarial esencial, teniendo en cuenta cualquier requisito de conservación de copias de archivo. La organización debería considerar la eliminación de información (ver 8.10) en medios de almacenamiento usados para copias de seguridad una vez que el período de conservación de la información expire y debería tener en cuenta la legislación y la normativa.

Otra información

Para más información sobre la seguridad del almacenamiento, incluida la consideración de la retención, ver norma ISO/IEC 27040.

8.14 Redundancia de instalaciones de tratamiento de información

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Availability	#Protect	#Continuity #Asset_ management	#Protection #Resilience

Control

Las instalaciones de procesamiento de información se deberían implementar con la redundancia suficiente para cumplir con requisitos de disponibilidad.

Propósito

Garantizar el funcionamiento continuo de instalaciones de procesamiento de información.

Guía

La organización debería identificar los requisitos de disponibilidad de los servicios empresariales y de los sistemas de información. La organización debería diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

La redundancia se puede introducir duplicando instalaciones de procesamiento de la información en parte o en su totalidad (por ejemplo, componentes de repuesto o tener dos de todo). La organización debería planificar y aplicar procedimientos para la activación de componentes e instalaciones de procesamiento redundantes. Los procedimientos deberían establecer si los componentes redundantes y actividades de procesamiento son siempre activados, o en caso de emergencia, activados automática o manualmente. Los componentes redundantes e instalaciones de procesamiento de la información deberían garantizar el mismo nivel de seguridad que los primarios.

Deberían existir mecanismos para alertar a la organización de cualquier fallo en instalaciones de procesamiento de información, que permitan ejecutar el procedimiento previsto y que permitan mantener disponibilidad mientras se reparan o sustituyen instalaciones de procesamiento de la información.

La organización debería tener en cuenta lo siguiente a la hora de implantar sistemas redundantes:

a) contratar a dos o más proveedores de instalaciones de red y de procesamiento de información crítica, como proveedores de servicios de Internet;

b) usar redes redundantes;

c) usar dos centros de datos separados geográficamente con sistemas duplicados;

d) usar fuentes de alimentación físicamente redundantes;

e) usar múltiples instancias paralelas de componentes de software, con un 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 las redes (por ejemplo, cortafuegos, rúters, conmutadores).

Según corresponda, preferentemente en modo de producción, los sistemas de información redundantes se deberían probar para garantizar que la conmutación por error de un componente a otro funcione según lo previsto.

Otra información

Existe una fuerte relación entre redundancia y preparación de ICT para la continuidad de actividad (ver 5.30), especialmente si se requieren tiempos de recuperación cortos. Muchas de las medidas de redundancia pueden formar parte de estrategias y soluciones de continuidad de ICT.

La implementación de redundancias puede introducir riesgos para la integridad (por ejemplo, los procesos de copia de datos en los componentes duplicados pueden introducir errores) o confidencialidad (por ejemplo, un control de seguridad débil de componentes duplicados puede llevar a un compromiso) de información y de sistemas de información, que se deberían considerar al diseñar sistemas de información.

La redundancia en las instalaciones de procesamiento de información no suele abordar la indisponibilidad de aplicaciones debido a fallos en las mismas.

Con el uso de la computación en nube pública, es posible tener múltiples versiones vivas de las instalaciones de procesamiento de información, que existen en múltiples ubicaciones físicas separadas con conmutación por error automática y equilibrio de carga entre ellas.

Algunas de tecnologías y técnicas para proporcionar redundancia y conmutación automática por error en el contexto de los servicios en la nube se argumentan en la norma ISO/IEC TS 23167.

8.15 Registro

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_ event_management	#Protection #Defence

Control

Se deberían producir, almacenar, proteger y analizar registros que graban actividades, excepciones, fallos y otros eventos relevantes.

Propósito

Para registrar eventos, generar pruebas, garantizar la integridad de información de registro, prevenir contra el acceso no autorizado, identificar los eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y apoyar las investigaciones.

Guía

Generalidades

La organización debería determinar el propósito para el que se crean los registros, qué datos se recopilan, registran y cualquier requisito específico de los registros para protegerlos y manejarlos. Esto se debería documentar en una política específica sobre registros.

Los registros de eventos deberían incluir para cada evento, según sea el caso:

a) identificaciones de usuario;

b) actividades de sistema;

c) fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión);

d) identidad del dispositivo, identificador de sistema y ubicación;

e) direcciones y protocolos de red.

Los siguientes eventos se deberían considerar para el registro:

a) intentos de acceso al sistema exitosos y rechazados;

b) intentos de acceso a los datos y a otros recursos, tanto los realizados con éxito como los rechazados;

c) cambios en la configuración de sistema;

d) uso de privilegios;

e) uso de programas y aplicaciones de utilidad;

f) archivos a los que se accedió y tipo de acceso, incluyendo el borrado de archivos de datos importantes;

g) alarmas emitidas por sistema de control de acceso;

h) activación y desactivación de los sistemas de seguridad, como los sistemas antivirus y los sistemas de detección de intrusos;

i) creación, modificación o supresión de identidades;

j) transacciones ejecutadas por usuarios en aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o gestionado 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, la alerta y la investigación de un incidente.

Protección de los registros

Los usuarios, incluidos los que tienen derechos de acceso privilegiados, no deberían tener permiso para borrar o desactivar registros de sus propias actividades. Pueden manipular potencialmente registros de instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de usuarios privilegiados.

Los controles deberían tener como objetivo proteger contra los cambios no autorizados en información de registro y problemas de funcionamiento con la instalación de registro, incluyendo:

a) alteraciones de los tipos de mensajes que se registran;

b) archivos de registro editados o borrados;

c) falta de registro de eventos o sobreescritura de eventos registrados anteriormente si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de registros, se debería considerar el uso de las siguientes técnicas: "hashing[9]"criptográfico, registro en un archivo de solo apéndice y de solo lectura, registro en un archivo de transparencia pública.

Se puede exigir el archivo de algunos registros de auditoría debido a los requisitos de conservación de datos o a los requisitos de recopilación y conservación de pruebas (ver 5.28).

En el caso de que la organización necesite enviar registros de sistema o de la aplicación a un proveedor para ayudar a depurar o solucionar errores, registros se deberían identificar en la medida de lo posible usando técnicas de enmascaramiento de datos (ver 8.11) para información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de servidor o nombre de la organización, antes de enviarlos al proveedor.

Los registros de eventos pueden contener datos sensibles e información personal identificable. Se deberían tomar medidas de protección de la privacidad adecuada (ver 5.34).

Análisis de registros

El análisis de registros debería abarcar el análisis y la interpretación de eventos de seguridad de información, para ayudar a identificar la actividad inusual o comportamiento anómalo, que pueden representar indicadores de compromiso.

El análisis de los acontecimientos se debería realizar teniendo en cuenta:

a) las competencias necesarias para los expertos que realizan el análisis;

b) determinación de procedimiento de análisis de los registros;

9 Del inglés hashing: *dispersión, método de dispersión, direccionamiento calculado o direccionamiento asociativo*.

c) los atributos necesarios de cada evento relacionado con la seguridad;

d) excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, reglas de gestión de información y eventos de seguridad (SIEM) o de cortafuegos y sistemas de detección de intrusiones (IDS) o firmas de “malware”];

e) patrones de comportamientos conocidos y el tráfico de red estándar en comparación con la actividad y comportamiento anómalos [análisis del comportamiento de usuarios y entidades (UEBA)];

f) resultados de análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de “big data[10]” y herramientas de análisis especializadas);

g) información disponible sobre las amenazas.

Los análisis de registros deberían estar respaldados por actividades de monitoreo específicas que ayuden a identificar y analizar comportamientos anómalos, lo que incluye:

a) revisar intentos exitosos y fallidos de acceso a los recursos protegidos [por ejemplo, servidores de sistema de nombres de dominio (DNS), portales Web y archivos compartidos];

b) comprobar registros de DNS para identificar las conexiones de red salientes a servidores maliciosos, como los asociados a los servidores de mando y control de las redes de “bots[11]“;

c) examinar informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicio) para detectar actividades inusuales en los sistemas y redes (por ejemplo, revisando los patrones de actividad);

d) incluir registros de eventos de vigilancia física, como entrada y salida, para garantizar una detección y un análisis de incidentes más precisos;

e) correlacionar registros para permitir un análisis eficaz y muy preciso.

Los incidentes de seguridad de la información presuntos y reales se deberían identificar (por ejemplo, infección de “malware” o sondeo de cortafuegos) y ser objeto de una investigación posterior (por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información, ver 5.25).

Otra información

Los registros de sistema suelen contener un gran volumen de información, mucha de la cual es ajena a la supervisión de seguridad de información. Para ayudar a identificar los eventos significativos para la supervisión de seguridad de la información, se puede considerar uso de programas de utilidad adecuados o herramientas de auditoría para realizar la interrogación de archivos.

El registro de eventos sienta las bases para sistemas de supervisión automatizados (ver 8.16) que son capaces de generar informes consolidados y alertas sobre seguridad de sistema.

10 Del inglés Big Data: *inteligencia de datos o ciencia de los datos.*

11 Del inglés bots: *zombi, ordenador zombi o bot.*

Una herramienta SIEM o un servicio equivalente se puede usar para almacenar, correlacionar, normalizar y analizar información de registros, así como para generar alertas. SIEM suelen requerir una minuciosa configuración para optimizar sus beneficios. Entre las configuraciones a tener en cuenta se encuentran la identificación y selección de las fuentes de registro adecuadas, el ajuste y las pruebas de las reglas y desarrollo de los casos de uso.

Los archivos públicos de transparencia para el registro de registros se usan, por ejemplo, en los sistemas de transparencia de certificados. Dichos archivos pueden proporcionar un mecanismo de detección adicional útil para estar protegido de la manipulación de los registros.

En los ambientes de nube, las responsabilidades de gestión de registros se pueden compartir entre el cliente del servicio de la nube y proveedor de servicios de la nube. Las responsabilidades varían en función del tipo de servicio en la nube que se use. En la norma ISO/IEC 27017 se pueden encontrar más orientaciones.

8.16 Actividades de monitoreo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_ event_management	#Defence

Control

Las redes, sistemas y aplicaciones se deberían supervisar para detectar comportamientos anómalos y tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Guía

El alcance y nivel de supervisión se deberían determinar de acuerdo con requisitos de empresa y de seguridad de la información, teniendo en cuenta leyes y reglamentos pertinentes. Registros de supervisión se deberían conservar durante períodos definidos.

Se debería considerar la inclusión de los siguientes elementos en sistema de control:

a) tráfico de salida y entrada de red, de sistema y de aplicaciones;

b) acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, otro;

c) archivos de configuración de sistema y de red de nivel crítico o de administrador;

d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros Web, cortafuegos, prevención de fugas de datos];

e) registros de eventos relacionados con actividad de sistema y de red;

f) comprobar que el código que se ejecuta está autorizado para funcionar en el sistema y que no fue manipulado (por ejemplo, mediante la recopilación para añadir código adicional no deseado);

g) uso de recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

La organización debería establecer una línea de base del comportamiento normal y supervisar contra esta línea de base para detectar anomalías. Al establecer una línea de base, se debería considerar lo siguiente:

a) revisión la utilización de sistemas en periodos normales y en periodos punta;

b) hora habitual de acceso, lugar de acceso, frecuencia de acceso para cada usuario o grupo de usuarios.

El sistema de supervisión se debería configurar con respecto a la línea de base establecida para identificar comportamientos anómalos, como, por ejemplo:

a) finalización imprevista de procesos o aplicaciones;

b) actividad típicamente asociada al “malware” o al tráfico procedente de direcciones IP o dominios de red maliciosos conocidos (por ejemplo, los asociados a servidores de mando y control de botnets);

c) características de ataques conocidos (por ejemplo, denegación de servicio y desbordamientos de búfer);

d) comportamiento inusual de sistema (por ejemplo, registro de pulsaciones, inyección de procesos y desviaciones en el uso de protocolos estándar);

e) cuellos de botella y sobrecargas (por ejemplo, colas en red, niveles de latencia y fluctuación de la red);

f) acceso no autorizado (real o intentado) a sistemas o información;

g) escaneo no autorizado de aplicaciones, sistemas y redes empresariales;

h) intentos exitosos y fallidos de acceso a recursos protegidos (por ejemplo, servidores DNS, portales Web y sistemas de archivos);

i) comportamiento inusual del usuario y de sistema en relación con el comportamiento esperado.

Se debería usar la supervisión continua mediante una herramienta de supervisión. La supervisión se debería realizar en tiempo real o en intervalos periódicos, según necesidades y capacidades de la organización. Las herramientas de monitorización deberían incluir la capacidad de manejar grandes cantidades de datos, adaptar un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también deberían ser capaces de reconocer firmas y datos específicos o patrones de comportamiento de la red o de las aplicaciones.

El “Software” de monitorización automatizada debería estar configurado para generar alertas (por ejemplo, a través de consolas de gestión, mensajes de correo electrónico o sistemas de mensajería instantánea) basadas en umbrales predefinidos. El sistema de alertas se debería ajustar y entrar en la línea base de la organización para minimizar falsos positivos. El personal debería estar dedicado a responder a las alertas y debería estar formado debidamente para interpretar con precisión los posibles incidentes. Debería haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los eventos anormales se deberían comunicar a partes relevantes para mejorar las siguientes actividades: auditoría, evaluación de la seguridad, escaneo de vulnerabilidades y monitoreo (ver 5.25). Se deberían establecer procedimientos para responder a indicadores positivos de sistema de monitoreo de manera oportuna, con el fin de minimizar el efecto de eventos adversos (ver 5.26) en seguridad de la información. También se deberían establecer procedimientos para identificar y tratar los falsos positivos, incluyendo el ajuste de “software” de monitorización para reducir el número de futuros falsos positivos.

Otra información

La supervisión de la seguridad se puede mejorar mediante:

a) aprovechamiento de sistemas de inteligencia sobre amenazas (ver 5.7);

b) aprovechamiento de capacidades de aprendizaje automático e inteligencia artificial;

c) utilización de listas de bloqueo o listas permitidas;

d) realización de una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ciberataques y ejercicios de ciberrespuesta), y usar los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable

e) utilización de sistemas de control de rendimiento para ayudar a establecer y detectar comportamientos anómalos;

f) aprovechamiento de registros en combinación con los sistemas de vigilancia.

Las actividades de monitoreo se suelen realizar mediante “software” especializado, como sistemas de detección de intrusos. Estos se pueden configurar para una línea de base de actividades normales, aceptables y esperadas de sistema y de red.

La monitorización de comunicaciones anómalas ayuda a identificar redes de “bots” (por ejemplo, un conjunto de dispositivos bajo el control malicioso del propietario de red de “bots”, que se suele usar para montar ataques de denegación de servicio distribuidos contra otros ordenadores de otras organizaciones). Si el ordenador está siendo controlado por un dispositivo externo, existe una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, la organización debería emplear tecnologías para supervisar comunicaciones anómalas y tomar medidas necesarias.

8.17 Sincronización de reloj

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Control

Los relojes de los sistemas de procesamiento de la información usados por la organización deberían estar sincronizados con las fuentes de tiempo aprobadas.

Propósito

Permitir correlación y análisis de eventos relacionados con seguridad y otros datos registrados y apoyar investigaciones sobre incidentes de seguridad de la información.

Guía

Los requisitos externos e internos para la representación del tiempo, sincronización fiable y precisión se deberían documentar y aplicar. Dichos requisitos pueden provenir de necesidades legales, estatutarias, reglamentarias, contractuales, normativas y de control interno. Se debería definir y considerar 1 h de referencia estándar para su uso dentro de la organización para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que se puedan 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) se debería usar como reloj de referencia para los sistemas de registro; una fuente de fecha y hora consistente y confiable para garantizar sellos de tiempo precisos. Se deberían usar 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 fiabilidad de los relojes externos y gestionar adecuadamente cualquier variación.

La sincronización del reloj puede ser difícil cuando se usan varios servicios en la nube o cuando se usan tanto servicios de esta como locales. En este caso, el reloj de cada servicio se debería supervisar y la diferencia registrada con el fin de mitigar riesgos derivados de discrepancias.

Otra información

La correcta configuración de relojes de computadores es importante para garantizar la exactitud de registros de eventos, que pueden ser necesarios para las investigaciones o como prueba en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dichas pruebas.

8.18 Uso de programas privilegiados de utilidad

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

Control

El uso de programas de utilidad que pueden ser capaces de anular los controles de sistema y de aplicación se debería restringir y controlar estrictamente.

Propósito

Garantizar que el uso de programas de utilidad no perjudique los controles de sistema y de las aplicaciones para seguridad de la información.

Guía

Se deberían tener en cuenta las siguientes directrices para uso de programas de utilidad que pueden ser capaces de anular los controles de sistema y de la aplicación:

a) limitación de uso de los programas de utilidad al mínimo número práctico de usuarios autorizados de confianza (ver 8.2);

b) uso de procedimientos de identificación, autenticación y autorización para los programas de servicios públicos, incluida la identificación única de la persona que utiliza el programa de servicios públicos;

c) definición y documentación de niveles de autorización de programas de servicios públicos;

d) autorización para uso "*ad hoc*" de programas de utilidad;

e) no colocación de programas de utilidad a disposición de usuarios que tienen acceso a aplicaciones en sistemas en los que se requiere segregación de funciones;

f) eliminación o desactivación todos los programas de utilidad innecesarios;

g) segregación lógica de programas de utilidad de "software" de aplicación, como mínimo. Cuando sea práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones;

h) limitación de la disponibilidad de los programas de servicios públicos (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todo el uso de los programas de utilidad.

Otra información

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden ser capaces de anular los controles de 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	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection

Control

Se deberían aplicar procedimientos y medidas para gestionar de forma segura la instalación de "software" en los sistemas operativos.

Propósito

Garantizar la integridad de los sistemas operativos y evitar la explotación de las vulnerabilidades técnicas.

Guía

Se deberían tener en cuenta las siguientes directrices para gestionar de forma segura los cambios y la instalación de "software" en los sistemas operativos:

a) realizar actualizaciones de "software" operativo solo por parte de administradores capacitados previa autorización de la dirección (ver 8.5);

b) garantizar que solo se instale en los sistemas operativos el código ejecutable aprobado y ningún código de desarrollo o compilador;

c) instalar y actualizar "software" solo después de haber realizado pruebas exhaustivas y satisfactorias (ver 8.29 y 8.31);

d) actualizar todas las bibliotecas de fuentes de programas correspondientes;

e) usar un sistema de control de la configuración para mantener control de todo "software" operativo, así como documentación de sistema;

f) definir una estrategia de reversión antes de aplicar cambios;

g) mantener un registro de auditoría de todas las actualizaciones de "software" operativo;

h) archivar versiones antiguas de "software", junto con toda información y parámetros necesarios, procedimientos, detalles de configuración y "software" de apoyo como medida de contingencia y mientras "software" sea necesario para leer o procesar los datos archivados.

Cualquier decisión de actualizar a una nueva versión debería tener en cuenta requisitos de empresa para el cambio y seguridad de versión (por ejemplo, la introducción de una nueva funcionalidad de seguridad de la información o número y gravedad de vulnerabilidades de seguridad de la información que afectan a la versión actual). Los parches de "software" se deberían aplicar cuando puedan ayudar a eliminar o reducir vulnerabilidades de seguridad de información (ver 8.8 y 8.19).

Los "Software" informáticos pueden depender del "software" y de paquetes suministrados externamente (por ejemplo, "software" programas que usan módulos que están alojados en sitios externos), que se deberían supervisar y controlar para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades en seguridad de información.

Un "Software" suministrado por el proveedor y usado en sistemas operativos se debería mantener en un nivel soportado por el proveedor. Con el tiempo, proveedores de "software" dejarán de dar soporte a versiones más antiguas de "software". La organización debería considerar los riesgos de confiar en "software" no soportado. "Software" de código abierto usado en los sistemas operativos se debería mantener hasta la última versión apropiada de "software". Con el tiempo, el código de fuente abierta se puede dejar de mantener, pero sigue estando disponible en un repositorio de "software" de fuente abierta. La organización también debería considerar riesgos de confiar en el "software" de código abierto no mantenido cuando se usa en sistemas operativos.

Cuando los proveedores participen en la instalación o actualización de programas informáticos, acceso físico o lógico solo se debería dar cuando sea necesario y con debida autorización. Las actividades de proveedor se deberían supervisar (ver 5.22).

La organización debería definir y aplicar normas estrictas sobre qué tipos de "software" pueden instalar los usuarios.

El principio de mínimo privilegio se debería aplicar a la instalación de "software" en sistemas operativos. La organización debería identificar qué tipos de instalaciones de "software" están permitidas (por ejemplo, actualizaciones y parches de seguridad para "software" existente) y qué tipos de instalaciones están prohibidas (por ejemplo, "software" que es solo para uso personal y "software" cuyo pedigrí con respecto a ser potencialmente malicioso es desconocido o sospechoso). Estos privilegios se deberían conceder en función de las atribuciones de usuarios afectados.

Otra información

Sin información.

8.20 Seguridad de redes

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

Control

Las redes y dispositivos de red deberían estar asegurados, gestionados y controlados para proteger información de sistemas y aplicaciones.

Propósito

Proteger información en redes y sus instalaciones de procesamiento de información de apoyo contra el compromiso a través de la red.

Guía

Se deberían implementar controles para garantizar seguridad de la información en redes y para proteger servicios conectados de acceso no autorizado. En particular, se deberían tener en cuenta los siguientes elementos:

a) el tipo y nivel de clasificación de información que puede soportar la red;

b) estableciendo responsabilidades y procedimientos para gestión de los equipos y dispositivos de red;

c) mantención de documentación actualizada, incluyendo diagramas de red y archivos de configuración de los dispositivos (por ejemplo, rúters, conmutadores);

d) separación de responsabilidad operativa de redes de operaciones de sistemas de ICT en que sea apropiado (ver 5.3);

e) implantación de controles para salvaguardar la confidencialidad e integridad de datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger sistemas y aplicaciones conectados (ver 5.22, 8.24, 5.14 y 6.6). También pueden ser necesarios controles adicionales para mantener disponibilidad de servicios de red y de computadores conectados a red;

f) registración y supervisión adecuadamente para permitir registro y detección de acciones que puedan afectar a seguridad de la información o que sean relevantes para ella (ver 8.16 y 8.15);

g) coordinación estrechamente de actividades de gestión de red, tanto para optimizar servicio a la organización como para garantizar que los controles se aplican de forma coherente en toda la infraestructura de procesamiento de información;

h) autenticación los sistemas en la red;

i) restricción y filtración de conexión de sistemas a la red (por ejemplo, usando cortafuegos);

j) detección, restricción y autenticación de conexión de equipos y dispositivos a la red;

k) endurecimiento de los dispositivos de red;

l) separación de canales de administración de red del resto de tráfico de esta;

m) aislamiento temporal de subredes críticas (por ejemplo, con puentes levadizos) si la red se está atacando;

n) desactivación de protocolos de red vulnerables.

La organización debería asegurar de que se aplican los controles de seguridad adecuados uso de redes virtualizadas. Las redes virtualizadas también abarcan redes definidas por “software” (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde punto de vista de seguridad, ya que pueden permitir separación lógica de la comunicación que tiene lugar a través de las redes físicas, en particular para sistemas y aplicaciones que se implementan usando la computación distribuida.

Otra información

Se puede encontrar información adicional sobre la seguridad de las redes en las normas ISO/IEC 27033.

Se puede encontrar más información sobre redes virtualizadas en la norma ISO/IEC TS 23167.

8.21 Seguridad de servicios de red

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red se deberían identificar, implementar y supervisar.

Propósito

Garantizar la seguridad en el uso de servicios de red.

Guía

Las medidas de seguridad necesarias para determinados servicios, como características de seguridad, niveles de servicio y requisitos de servicio, se deberían identificar e implementar (por proveedores de servicios de red internos o externos). La organización debería garantizar que proveedores de servicios de red apliquen estas medidas.

La capacidad del proveedor de servicios de red para gestionar servicios acordados de forma segura se debería determinar y supervisar periódicamente. La organización y proveedor deberían acordar el derecho de auditoría. La organización también debería tener en cuenta las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Se deberían formular y aplicar normas sobre uso de redes y servicios de red para cubrir:

a) las redes y los servicios de red a los que se puede 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) gestión de red, controles, procedimientos tecnológicos para proteger el acceso a conexiones y servicios de red;

e) medios usados para acceder a las redes y a los servicios de red [por ejemplo, el uso de una red privada virtual (VPN) o de una red inalámbrica];

f) hora, ubicación y otros atributos del usuario en el momento de acceso;

g) supervisión de uso de servicios de red.

Se deberían tener en cuenta las siguientes características de seguridad de los servicios de red:

a) tecnología aplicada para la seguridad de los servicios de red, como la autenticación, el cifrado y controles de conexión a red;

b) parámetros técnicos necesarios para la conexión segura con servicios de red, de acuerdo con normas de seguridad y de conexión a red;

c) almacenamiento en caché (por ejemplo, en una red de entrega de contenidos) y sus parámetros que permiten a usuarios elegir el uso de la caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad;

d) procedimientos para el uso del servicio de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

Otra información

Los servicios de red incluyen suministro de conexiones, servicios de red privada y soluciones de seguridad de red gestionadas, como cortafuegos y sistemas de detección de intrusiones. Estos servicios pueden ir desde un simple ancho de banda no gestionado hasta complejas ofertas de valor añadido.

En la norma ISO/IEC 29146 se ofrecen más orientaciones sobre un marco para gestión de acceso.

8.22 Segregación de redes

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control

Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en las redes de la organización.

Propósito

Dividir red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de la empresa.

Guía

La organización debería considerar gestión de la seguridad de grandes redes dividiéndolas en dominios de red separados y segregándolas de la red pública (por ejemplo, Internet). Los dominios se pueden elegir en función de niveles de confianza, criticidad y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de bajo y alto riesgo), a lo largo de las unidades organizativas (por ejemplo, recursos humanos, finanzas y mercadotecnia) o alguna combinación (por ejemplo, dominio de servidor que se conecta a múltiples unidades organizativas). La segregación se puede hacer usando redes físicamente diferentes o usando redes lógicas diferentes.

El perímetro de cada dominio debería estar bien definido. Si se permite el acceso entre dominios de red, se debería controlar en el perímetro mediante una pasarela (por ejemplo, cortafuegos, rúter de filtrado). Los criterios para la segregación de redes en dominios y acceso permitido a través de pasarelas, se debería basar en una evaluación de requisitos de seguridad de cada dominio. La evaluación debería estar en consonancia con la política específica de control de acceso (ver 5.15), requisitos de acceso, valor y clasificación de información procesada y tener en cuenta el coste relativo e impacto en rendimiento de incorporación de una tecnología de pasarela adecuada.

Las redes inalámbricas requieren un tratamiento especial debido a la escasa definición del perímetro de la red. Se debería considerar el ajuste de la cobertura radioeléctrica para la segregación de redes inalámbricas. En el caso de entornos sensibles, se debería considerar la posibilidad de tratar todos los accesos inalámbricos como conexiones externas y segregar este acceso de redes internas hasta que acceso haya pasado por una pasarela de acuerdo con los controles de red (ver 8.20) antes de conceder acceso a los sistemas internos. Red de acceso inalámbrico para invitados debería estar segregada de la del personal si este solo usa dispositivos terminales de usuario controlados que cumplan con políticas específicas de la organización. El WiFi para invitados debería tener al menos las mismas restricciones que el WiFi para el personal, con el fin de desalentar el uso de WiFi para invitados por parte del personal.

Otra información

Las redes a menudo se extienden más allá de los límites de la organización ya que se forman asociaciones empresariales que requieren la interconexión o el uso compartido de instalaciones de procesamiento de información y de redes. Estas 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 Filtro Web

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control

El acceso a sitios Web externos se debería gestionar para reducir exposición a contenidos maliciosos.

Propósito

Para proteger sistemas de ser comprometidos por el “malware” y para prevenir acceso a recursos Web no autorizados.

Guía

La organización debería reducir los riesgos de que su personal acceda a sitios Web que contienen información ilegal o que se sabe que contienen virus o material de phishing. Una técnica para conseguirlo consiste en bloquear la dirección IP o el dominio del sitio o sitios Web en cuestión. Algunos navegadores y tecnologías antimalware lo hacen automáticamente o se pueden configurar para ello.

La organización debería identificar los tipos de sitios Web a los que el personal debería o no tener acceso. La organización debería considerar el bloqueo de acceso a los siguientes tipos de sitios Web:

a) sitios Web que tienen una función de carga de información, a menos que se permita por razones comerciales válidas;

b) sitios Web conocidos o sospechosos de ser maliciosos (por ejemplo, los que distribuyen "malware" o contenidos de "phishing[12]");

c) servidores de mando y control;

d) sitio Web malicioso adquirido de la inteligencia de amenazas (ver 5.7);

e) sitios Web que comparten contenidos ilegales.

Antes de desplegar este control, la organización debería establecer reglas para uso seguro y apropiado de recursos en línea, incluyendo cualquier restricción a sitios Web y aplicaciones basadas en la Web indeseables o inapropiadas. Las normas se deberían mantener actualizadas.

Se debería impartir formación al personal sobre uso seguro y adecuado de los recursos en línea, incluido el acceso a la Web. La formación debería incluir las normas de la organización, punto de contacto para plantear problemas de seguridad y proceso de excepción en que los recursos Web restringidos necesitan acceder por razones de negocio legítimas. La formación también se debería impartir al personal para garantizar que no anulan ningún aviso del navegador que informe de que un sitio Web no es seguro pero que permite al usuario continuar.

Otra información

El filtro Web puede incluir una serie de técnicas que incluyen firmas, heurística, lista de sitios Web o dominios aceptables, lista de sitios Web o dominios prohibidos y configuración a medida para ayudar a evitar que el "software" malicioso y otras actividades maliciosas ataquen red y sistemas de la organización.

8.24 Uso de criptografía

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

12 Del inglés phishing: *phishing, ataque por suplantación de identidad o captación ilegítima de datos confidenciales.*

Control

Se deberían definir y aplicar normas para uso eficaz de la criptografía, incluida gestión de claves criptográficas.

Propósito

Garantizar uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos empresariales, de seguridad de la información y teniendo en cuenta requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Guía

Generalidades

Al utilizar la criptografía, se debería considerar lo siguiente:

a) la política específica sobre criptografía definida por la organización, incluyendo los principios generales para la protección de la información. Es necesario contar con una política específica sobre uso de la criptografía para maximizar los beneficios y minimizar los riesgos de uso de las técnicas criptográficas y para evitar un uso inapropiado o incorrecto;

b) identificación de nivel de protección requerido y clasificación de información y, en consecuencia, establecer tipo, fuerza y calidad de algoritmos criptográficos necesarios;

c) el uso de criptografía para protección de información contenida en dispositivos finales de los usuarios móviles o en medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;

d) el enfoque de gestión de claves, incluidos los métodos para tratar la generación y protección de claves criptográficas y recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves;

e) funciones y responsabilidades para:

   1) la aplicación de las normas para uso eficaz de criptografía;

   2) la gestión de claves, incluyendo la generación de claves (ver 8.24);

f) las normas se adoptan, así como los algoritmos criptográficos, potencia de cifrado, soluciones criptográficas y prácticas de uso que se aprueben o requieran para su utilización en la organización;

g) el impacto de uso de información cifrada en los controles que dependen de la inspección de contenidos (por ejemplo, detección de “malware” o filtrado de contenidos).

Cuando la aplicación de normas de la organización para el uso efectivo de la criptografía, se deberían tener en cuenta regulaciones y restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo, así como cuestiones de flujo transfronterizo de información cifrada (ver 5.31).

El contenido de acuerdos de nivel de servicio o de contratos con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) debería cubrir cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta para la prestación de estos (ver 5.22).

Administración de claves

La administración adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir las claves criptográficas.

Un sistema de administración de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generación claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) emisión y obtención de certificados de clave pública;

c) distribución de claves a entidades previstas, incluyendo la forma de activar claves en que se reciben;

d) mantención de claves, incluido el modo en que los usuarios autorizados obtienen acceso a las mismas;

e) cambio o actualización de claves, incluyendo normas sobre en que cambiar claves y cómo se hará;

f) tratamiento de las claves comprometidas;

g) revocación de claves, incluyendo el modo de retirarlas o desactivarlas [por ejemplo, cuando las claves se vieron comprometidas o en que un usuario abandona la organización (en cuyo caso las claves también se deberían archivar)];

h) recuperación de claves perdidas o dañadas;

i) copia de seguridad o archivo de claves;

j) destrucción de claves;

k) registro y audición de actividades clave relacionadas con gestión;

l) fijación de fechas de activación y desactivación de claves, de modo que estas solo se puedan usar durante el período de tiempo previsto en normas de la organización sobre gestión de claves;

m) gestión de solicitudes legales de acceso a claves criptográficas (por ejemplo, se puede exigir que la información encriptada esté disponible en forma no encriptada como prueba en un caso judicial).

Todas las claves criptográficas deberían estar protegidas contra modificación y pérdida. Además, claves secretas y privadas deben estar protegidas contra uso no autorizado y divulgación. Equipo usado para generar, almacenar y archivar claves debería estar protegido físicamente.

Además de la integridad, para muchos casos de uso, también se debería considerar la autenticidad de claves públicas.

Otra información

La autenticidad de claves públicas se suele abordar mediante procesos de gestión de claves públicas que usan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante tecnologías como aplicación de procesos manuales para claves de pequeño número.

La criptografía se puede usar para alcanzar diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: uso de la encriptación de la información para proteger la información sensible o crítica, ya sea almacenada o transmitida;

b) integridad o autenticidad: utilización de firmas digitales o códigos de autenticación de mensajes para verificar autenticidad o integridad de información sensible o crítica almacenada o transmitida. Utilización de algoritmos para la comprobación de integridad de archivos;

c) no repudio: uso de técnicas criptográficas para proporcionar evidencia de la ocurrencia o no de un evento o acción;

d) autenticación: uso de técnicas criptográficas para autenticar a los usuarios y otras entidades de sistema que solicitan acceso o realizan transacciones con usuarios, entidades y recursos de sistema.

Las normas ISO/IEC 11770 ofrecen más información sobre gestión de claves.

8.25 Ciclo de vida de desarrollo seguro

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_ security	#Protection

Control

Se deberían establecer y aplicar normas para desarrollo seguro de “software” y sistemas.

Propósito

Garantizar que seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de “software” y sistemas.

Guía

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un “software” y un sistema seguro. Para conseguirlo, se deberían considerar los siguientes aspectos:

a) separación de entornos de desarrollo, prueba y producción (ver 8.31);

b) guía sobre seguridad en el ciclo de vida de desarrollo de “software”:

   1) seguridad en metodología de desarrollo de “software” (ver 8.28 y 8.27);

2) directrices de codificación segura para cada lenguaje de programación usado (ver 8.28);

c) requisitos de seguridad en la fase de especificación y diseño (ver 5.8);

d) controles de seguridad en proyectos (ver 5.8);

e) pruebas de sistema y de seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración (ver 8.29);

f) repositorios seguros para código fuente y configuración (ver 8.4 y 8.9);

g) seguridad en el control de versiones (ver 8.32);

h) conocimientos y formación en materia de seguridad de las aplicaciones (ver 8.28);

i) capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (ver 8.28);

j) requisitos de licencia y las alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (ver 5.32).

Si desarrollo se subcontrata, la organización debería obtener garantías de que el proveedor cumple con las normas de la organización para desarrollo seguro (ver 8.30).

Otra información

El desarrollo también puede tener lugar dentro de aplicaciones, como ofimáticas, scripts, navegadores y bases de datos.

8.26 Requisito de Seguridad de las aplicaciones

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence

Control

Los requisitos de seguridad de información se deberían identificar, especificar y aprobar en que desarrollar o adquirir aplicaciones.

Propósito

Garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

Guía

Generalidades

Los requisitos de seguridad de aplicaciones se deberían identificar y especificar. Estos requisitos se suelen determinar mediante una evaluación de riesgos. Los requisitos se deberían desarrollar con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de aplicaciones pueden abarcar un amplio abanico de temas, dependiendo del propósito de la aplicación.

Los requisitos de seguridad de aplicación deberían incluir, según sea el caso:

a) nivel de confianza en la identidad de las entidades [por ejemplo, mediante la autenticación (ver 5.17, 8.2 y 8.5)];

b) identificar el tipo de información y el nivel de clasificación que debería procesar la aplicación;

c) necesidad de segregación de acceso y nivel de acceso a los datos y funciones de la aplicación;

d) resiliencia frente a ataques malintencionados o interrupciones involuntarias [por ejemplo, protección contra el desbordamiento de búfer o inyecciones de lenguaje de consulta estructurado (SQL)];

e) requisitos legales, estatutarios y reglamentarios de la jurisdicción donde se genera, procesa, completa o almacena la transacción;

f) necesidad de privacidad asociada a todas las partes implicadas;

g) los requisitos de protección de cualquier información confidencial;

h) protección de datos durante su tratamiento, en tránsito y en reposo;

i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes implicadas;

j) controles de entrada, incluidas las comprobaciones de integridad y validación de entradas;

k) controles automatizados (por ejemplo, límites de aprobación o dobles aprobaciones);

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 "free-text[13]", ya que pueden dar lugar a un almacenamiento incontrolado de datos confidenciales (por ejemplo, datos personales);

n) requisitos derivados del proceso de negocio, como el registro y supervisión de transacciones, requisitos de no repudio;

o) requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces con sistemas de registro y supervisión o de detección de fugas de datos);

p) gestión de mensajes de error.

Servicios transaccionales

Además, en caso de aplicaciones que ofrecen servicios transaccionales entre la organización y un socio, al identificar los requisitos de seguridad de la información se debería considerar lo siguiente:

a) nivel de confianza que cada parte requiere en la identidad declarada de la otra;

13 Del inglés free-text: *mensaje de contenido libre o texto libre*.

b) nivel de confianza requerido en integridad de información intercambiada o procesada y los mecanismos de identificación de falta de integridad (por ejemplo, comprobación de redundancia cíclica, “hashing”, firmas digitales);

c) procesos de autorización asociados a quién puede aprobar contenido de documentos transaccionales clave, emitirlos o firmarlos;

d) confidencialidad, integridad, prueba del envío y recepción de documentos clave y no repudio (por ejemplo, contratos asociados a procesos de licitación y contratación);

e) confidencialidad e integridad de cualquier transacción (por ejemplo, pedidos, datos de la dirección de entrega y confirmación de recibos);

f) requisitos sobre el tiempo que se debería mantener la confidencialidad de una transacción;

g) seguros y otros requisitos contractuales.

Aplicaciones de pedidos y pagos electrónicos

Además, en caso de aplicaciones que implican pedidos y pagos electrónicos, se debería tener en cuenta lo siguiente:

a) requisitos para mantener la confidencialidad e integridad de información de pedidos;

b) grado de verificación apropiado para comprobar la información de pago suministrada por un cliente;

c) evitación de pérdida o duplicación de información de transacciones;

d) almacenamiento de detalles de transacciones fuera de cualquier entorno de acceso público (por ejemplo, en una plataforma de almacenamiento existente en intranet de la organización, no conservada y expuesta en medios de almacenamiento electrónico directamente accesibles desde internet);

e) seguridad está integrada en todo proceso de gestión de certificados o firmas en que se usa una autoridad de confianza (por ejemplo, para emisión y mantenimiento de firmas o certificados digitales).

Varias de las consideraciones anteriores se pueden abordar mediante la aplicación de criptografía (ver 8.24), teniendo en cuenta los requisitos legales (ver 5.31 a 5.36, especialmente ver 5.31 para legislación sobre criptografía).

Otra información

Las aplicaciones accesibles a través de redes están sujetas a una serie de amenazas relacionadas con la red, como actividades fraudulentas, conflictos contractuales o la divulgación de información al público; transmisión incompleta, desvío, alteración no autorizada de mensajes, duplicación o repetición. Por lo tanto, es indispensable realizar evaluaciones detalladas de riesgos y determinar, de manera cautelosa, los controles. Los controles necesarios suelen incluir métodos criptográficos para autenticación y seguridad de la transferencia de datos.

Se puede encontrar más información sobre la seguridad de las aplicaciones en la norma ISO/IEC 27034.

8.27 Principios de ingeniería y arquitectura de sistemas seguros

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control

Los principios para la ingeniería de sistemas seguros se deberían establecer, documentar, mantener y aplicar a cualquier actividad de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida de desarrollo.

Guía

Los principios de ingeniería de seguridad se deberían establecer, documentar y aplicar a las actividades de ingeniería de los sistemas de información. La seguridad se debería diseñar en todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología). La nueva tecnología se debería analizar en cuanto a riesgos de seguridad y diseño se debería revisar con respecto a patrones de ataque conocidos.

Los principios de ingeniería de seguridad orientan sobre las técnicas de autenticación de usuarios, control de sesiones seguras, validación y saneamiento de datos.

Los principios de ingeniería de sistemas seguros deberían incluir el análisis de:

a) información y sistemas contra las amenazas identificadas, toda la gama de controles de seguridad necesarios para proteger;

b) capacidad de los controles de seguridad para prevenir, detectar o responder a eventos de seguridad;

c) controles de seguridad específicos requeridos por determinados procesos empresariales (por ejemplo, cifrado de información sensible, comprobación de la integridad y firma digital de la información);

d) dónde y cómo se deberían aplicar los controles de seguridad (por ejemplo, mediante la integración con una arquitectura de seguridad y la infraestructura técnica);

e) cómo funcionan los controles de seguridad individuales (manuales y automatizados) para producir un conjunto integrado de controles.

Los principios de ingeniería de seguridad deberían tener en cuenta:

a) necesidad de integrar una arquitectura de seguridad;

b) infraestructura técnica de seguridad [por ejemplo, infraestructura de clave pública (PKI), la gestión de identidades y accesos (IAM), prevención de fuga de datos y gestión dinámica de los accesos];

c) capacidad de la organización para desarrollar y apoyar la tecnología elegida;

d) coste, tiempo y complejidad del cumplimiento de requisitos de seguridad;

e) buenas prácticas actuales.

La ingeniería de sistemas seguros debería implicar:

a) el uso de los principios de la arquitectura de seguridad, tales como “security by design”, “defence in depth”, “security by default”, “default deny”, “fail securely”, “distrust input from external applications”, “security in deployment”, “assume breach”, “least privilege”, “usability and manageability” y “least functionality”;

b) una revisión del diseño orientada a la seguridad para ayudar a identificar vulnerabilidades de seguridad de información, garantizar que se especifican controles de seguridad y cumplir con requisitos de seguridad;

c) la documentación y reconocimiento formal de controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad imperativos);

d) el endurecimiento de los sistemas.

La organización debería considerar principios de “zero trust[14]” como:

a) asumir que sistemas de información de la organización ya se vulneraron y, por tanto, no depender únicamente de la seguridad de perímetro de red;

b) emplear un enfoque de “never trust and always verify” para acceso a sistemas de información;

c) garantizar que solicitudes a sistemas de información estén cifradas de extremo a extremo;

d) verificar cada solicitud a un sistema de información como si se originara en una red abierta y externa, incluyendo si estas solicitudes se originan dentro de la organización (por ejemplo, no confiar automáticamente en nada dentro o fuera de sus perímetros);

e) usar técnicas de control de acceso dinámico y de “least privilege[15]” (ver 5.15, 5.18 y 8.2). Esto incluye autenticación y autorización de solicitudes de información o a sistemas sobre la base de información contextual, como información de autenticación (ver 5.17), identidades de usuarios (ver 5.16), datos sobre el dispositivo terminales del usuario y clasificación de datos (ver 5.12);

f) autenticar siempre a solicitantes y validar siempre solicitudes de autorización a los sistemas de información sobre la base de información que incluya información de autenticación (ver 5.17) e identidades de usuarios (5.16), datos sobre dispositivo terminal del usuario y clasificación de datos (ver 5.12), por ejemplo, aplicando una autenticación fuerte (por ejemplo, multifactor, ver 8.5).

14 Del inglés zero trust: *confianza cero*.

15 Del inglés least privilege: *principio del mínimo privilegio u operar con los privilegios mínimos.*

Los principios de ingeniería de seguridad establecidos se deberían aplicar, en que, al desarrollo externalizado de sistemas de información a través de los contratos y otros acuerdos vinculantes entre la organización y el proveedor al que se subcontrata. La organización se debería asegurar de que las prácticas de ingeniería de seguridad de los proveedores se ajustan a las necesidades de la organización.

Los principios de ingeniería de seguridad y procedimientos de ingeniería establecidos se deberían revisar regularmente para garantizar que contribuyen efectivamente a mejorar los estándares de seguridad dentro del proceso de ingeniería. Periódicamente se deberían revisar también para garantizar que se mantienen actualizados en lo que respecta a la lucha contra cualquier nueva amenaza potencial y para que sigan siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Otra información

Los principios de ingeniería de seguridad se pueden aplicar al diseño o configuración de una serie de técnicas, como:

— tolerancia a fallos y otras técnicas de resiliencia;

— segregación (por ejemplo, a través de virtualización o contenedorización);

— resistencia a la manipulación.

Se pueden utilizar técnicas de virtualización segura para evitar interferencia entre aplicaciones que se ejecutan en el mismo dispositivo físico. Si una instancia virtual de una aplicación es comprometida por un atacante, solo esa instancia se ve afectada. El ataque no tiene efecto sobre ninguna otra aplicación o datos.

Se pueden utilizar técnicas de resistencia a manipulación para detectar manipulación de contenedores de información, ya sean físicos (por ejemplo, una alarma antirrobo) o lógicos (por ejemplo, un archivo de datos). Una característica de estas técnicas es que queda constancia del intento de manipulación del contenedor. Además, el control puede impedir la extracción con éxito de datos mediante su destrucción (por ejemplo, se puede borrar la memoria del dispositivo).

8.28 Codificación segura

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control

Los principios de codificación segura se deberían aplicar al desarrollo de “software”.

Propósito

Garantizar que el “software” se escribe de forma segura, reduciendo así el número de posibles vulnerabilidades de seguridad de la información en el “software”.

Guía

Generalidades

La organización debería establecer procesos en toda la estructura para proporcionar una buena gobernanza para la codificación segura. Se debería establecer y aplicar una línea de base segura mínima. Además, dichos procesos y gobernanza se deberían ampliar para cubrir los componentes de "software" de terceros y "software" de código abierto.

La organización debería supervisar amenazas del mundo real y consejos e información actualizados sobre vulnerabilidades de "software" para guiar los principios de codificación segura de la organización a través de la mejora y aprendizaje continuos. Esto puede ayudar a garantizar que se apliquen prácticas de codificación seguras y eficaces para combatir el panorama cambiante de amenazas.

Planificación y antes de la codificación

Los principios de codificación segura se deberían usar tanto en nuevos desarrollos como en escenarios de reutilización. Estos principios se deberían aplicar a actividades de desarrollo tanto dentro de la organización como para productos y servicios suministrados por la organización a otros. Planificación y requisitos previos a la codificación deberían incluir:

a) expectativas específicas de la organización y principios aprobados para codificación segura que se usarán tanto para los desarrollos de código internos como externos;

b) prácticas de codificación comunes e históricas y defectos que conducen a vulnerabilidades de la seguridad de información;

c) configuración de herramientas de desarrollo, como entornos de desarrollo integrados (IDE), para ayudar a imponer la creación de código seguro;

d) monitoreo de orientaciones emitidas por proveedores de herramientas de desarrollo y entornos de ejecución, según proceda;

e) mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores);

f) cualificación de los desarrolladores en la escritura de código seguro;

g) diseño y arquitectura seguros, incluida la modelización de amenazas;

h) normas de codificación seguras y en que sea pertinente exigir su uso;

i) uso de entornos controlados para desarrollo.

Durante la codificación

Las consideraciones durante la codificación deberían incluir:

a) prácticas de codificación seguras específicas de los lenguajes y técnicas de programación que se usan;

b) uso de técnicas de programación segura, como la programación por parejas, la refactorización, la revisión por pares, las iteraciones de seguridad y desarrollo basado en pruebas;

c) uso de técnicas de programación estructurada;

d) documentación del código y eliminación de defectos de programación, que pueden permitir la explotación de vulnerabilidades de seguridad de la información;

e) prohibición de uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, muestras de código no aprobadas y servicios Web no autenticados).

Se deberían realizar pruebas durante y después de desarrollo (ver 8.29). Los procesos de pruebas estáticas de seguridad de las aplicaciones (SAST) pueden identificar vulnerabilidades de seguridad en el "software".

Antes de poner en funcionamiento el "software", se debería evaluar lo siguiente:

a) principio del mínimo privilegio y superficie de ataque;

b) realización de análisis de errores de programación más comunes y documentar que se mitigaron.

Revisión y mantenimiento

Después de que el código se hizo operativo:

a) actualizaciones deberían estar empaquetadas y desplegadas de forma segura;

b) vulnerabilidades de seguridad de información notificadas se deberían tratar (ver 8.8);

c) errores y sospechas de ataques se deberían registrar y estos se deberían revisar regularmente para realizar los ajustes necesarios en el código;

d) código fuente debería estar protegido contra acceso no autorizado y manipulación (por ejemplo, mediante el uso de herramientas de gestión de configuración, que suelen ofrecer funciones como control de acceso y de versiones).

Si se usan herramientas y bibliotecas externas, la organización debería tener en cuenta:

a) garantía de gestión de bibliotecas externas (por ejemplo, manteniendo un inventario de las bibliotecas usadas y sus versiones) y su actualización periódica con los ciclos de publicación;

b) selección, autorización y reutilización de componentes bien probados, en particular componentes de autenticación y criptográficos;

c) licencia, seguridad e historial de componentes externos;

d) garantía que el "software" se pueda mantener, seguir su pista y que proceda de fuentes acreditadas y reputadas;

e) disponibilidad a largo plazo de recursos y artefactos de desarrollo.

Cuando un paquete de "software" se necesita modificar, los siguientes puntos se deberían considerar:

a) el riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos;

b) si se obtiene 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) la compatibilidad con otros "software" en uso.

Otra información

Un principio rector es garantizar que el código relevante para seguridad se invoque cuando sea necesario y sea resistente a manipulaciones. Los programas instalados a partir de código binario compilado también tienen estas propiedades, pero solo para los datos contenidos en la aplicación. En el caso de los lenguajes interpretados, el concepto solo funciona cuando el código se ejecuta en un servidor inaccesible para usuarios y procesos que lo usan y que sus datos se guardan en una base de datos igualmente protegida. Por ejemplo, el código interpretado se puede ejecutar en un servicio en la nube en que acceso al propio código requiere privilegios de administrador. Este acceso de administrador debería estar protegido por mecanismos de seguridad como los principios de administración "just-in-time[16]" y autenticación fuerte. Si el propietario de la aplicación puede acceder a los scripts mediante un acceso remoto directo al servidor, en principio también puede hacerlo un atacante. Servidores Web deberían estar configurados para impedir navegación por los directorios en estos casos.

La mejor manera de diseñar el código de las aplicaciones es partiendo de la base de que siempre está sujeto a ataques, por error o por acción maliciosa. Además, las aplicaciones críticas se pueden diseñar para ser tolerantes a fallos internos. Por ejemplo, la salida de un algoritmo complejo se puede comprobar para asegurar que se encuentra dentro de los límites de seguridad antes de que los datos se usen en una aplicación como una aplicación crítica de seguridad o financiera. El código que realiza comprobaciones de límites es sencillo y, por tanto, mucho más fácil de demostrar su corrección.

Algunas aplicaciones Web son susceptibles de sufrir una serie de vulnerabilidades introducidas por un diseño y una codificación deficientes, como la inyección en la base de datos y los ataques de scripting entre sitios. En estos ataques, las peticiones se pueden manipular para abusar de la funcionalidad del servidor Web.

Se puede encontrar más información sobre la evaluación de la seguridad de ICT en la norma ISO/IEC 15408.

8.29 Pruebas de seguridad en desarrollo y aceptación

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection

16 Del inglés just-in-time: *justo a tiempo, JIT, fabricación justo a tiempo o carácter "puntual"*.

Control

Los procesos de pruebas de seguridad se deberían definir e implementar en el ciclo de vida de desarrollo.

Propósito

Validar si se cumplen requisitos de seguridad de información cuando las aplicaciones o código se despliegan en entorno de producción.

Guía

Los nuevos sistemas de información, actualizaciones y nuevas versiones se deberían probar y verificar a fondo durante procesos de desarrollo. Las pruebas de seguridad deberían ser una parte integral de pruebas de los sistemas o componentes.

Las pruebas de seguridad se deberían realizar en función de un conjunto de requisitos, que se pueden expresar como funcionales o no funcionales. Pruebas de seguridad deberían incluir pruebas de:

a) funciones de seguridad [por ejemplo, autenticación de usuarios (ver 8.5), restricción de acceso (ver 8.3) y uso de criptografía (ver 8.24)];

b) codificación segura (ver 8.28);

c) configuraciones seguras (ver 8.9, 8.20 y 8.22), incluyendo la de sistemas operativos, cortafuegos y otros componentes de seguridad.

Los planes de prueba se deberían determinar usando un conjunto de criterios. Los alcances de pruebas deberían ser proporcional a la importancia, la naturaleza de sistema y el impacto potencial del cambio que se introduce. El plan de pruebas debería incluir:

a) calendario detallado de actividades y pruebas;

b) insumos y resultados previstos en una serie de condiciones;

c) criterios para evaluar los resultados;

d) decisión de emprender otras acciones en caso necesario.

La organización puede aprovechar herramientas automatizadas, como las de análisis de código o escáneres de vulnerabilidad y debería verificar la corrección de defectos relacionados con seguridad.

En el caso de los desarrollos internos, estas pruebas se deberían realizar inicialmente por el equipo de desarrollo. A continuación, se deberían realizar pruebas de aceptación independientes para garantizar que el sistema funciona como se espera y solo como se espera (ver 5.8). Se debería tener en cuenta lo siguiente:

a) realizar actividades de revisión del código como elemento relevante para comprobación de fallos de seguridad, incluyendo entradas y condiciones no previstas;

b) realizar escaneos de vulnerabilidad para identificar configuraciones inseguras y vulnerabilidades de sistema;

c) realizar pruebas de penetración para identificar el código y el diseño inseguros.

En el caso de los componentes de desarrollo y compra subcontratados, se debería seguir un proceso de adquisición. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados (ver 5.20). Los productos y servicios se deberían evaluar según estos criterios antes de su adquisición.

Las pruebas se deberían realizar en un entorno de pruebas que se asemeje lo más posible al entorno de producción objetivo para garantizar que el sistema no introduce vulnerabilidades en el entorno de la organización y que las pruebas son fiables (ver 8.31).

Otra información

Se pueden establecer múltiples entornos de prueba, que se pueden usar 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 debe tener en cuenta las pruebas y supervisión de entornos de prueba, herramientas y tecnologías para garantizar eficacia de las pruebas. Las mismas consideraciones se aplican a la supervisión de sistemas de control desplegados en entornos de desarrollo, prueba y producción. Es necesario tener criterio, guiado por la sensibilidad de sistemas y datos, para determinar cuántas capas de meta pruebas son útiles.

8.30 Desarrollo externo

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

La organización debería dirigir, supervisar y revisar las actividades relacionadas con desarrollo de sistemas subcontratados.

Propósito

Garantizar la aplicación de las medidas de seguridad de la información requeridas por la organización en desarrollo de sistemas subcontratados.

Guía

Cuando el desarrollo de sistema se externaliza, la organización debería comunicar y acordar requisitos y expectativas, supervisar y revisar continuamente si la entrega del trabajo externalizado cumple con estas expectativas. Los siguientes puntos se deberían considerar en toda la cadena de suministro externa de la organización:

a) acuerdos de licencia, titularidad de código y derechos de propiedad intelectual relacionados con los contenidos subcontratados (ver 5.32);

b) requisitos contractuales para prácticas de diseño, codificación y pruebas seguras (ver 8.25 a 8.29);

c) suministro del modelo de amenaza a considerar por desarrolladores externos;

d) pruebas de aceptación de la calidad y la precisión de los resultados (ver 8.29);

e) presentación de pruebas que establecieron niveles mínimos aceptables de capacidades de seguridad y privacidad (por ejemplo, informes de garantía);

f) presentación de pruebas que se realizaron pruebas suficientes para evitar la presencia de contenidos maliciosos (tanto intencionados como no intencionados) en el momento de la entrega;

g) presentación de pruebas de que se han realizado suficientes pruebas para evitar la presencia de vulnerabilidades conocidas;

h) acuerdos de custodia del código fuente del "software" (por ejemplo, si el proveedor quiebra);

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, en materia de protección de datos personales).

Otra información

Se puede encontrar más información sobre relaciones con proveedores en la norma ISO/IEC 27036.

8.31 Separación de entornos de desarrollo, prueba y producción

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control

Entornos de desarrollo, pruebas y producción deberían estar separados y asegurados.

Propósito

Proteger el entorno de producción y datos de riesgos derivados de actividades de desarrollo y prueba.

Guía

Se debería identificar e implementar el nivel de separación entre entornos de producción, pruebas y desarrollo que es necesario para evitar problemas de producción.

Se deberían tener en cuenta los siguientes puntos:

a) separar adecuadamente los sistemas de desarrollo y de producción y hacerlos funcionar en dominios diferentes (por ejemplo, en entornos virtuales o físicos separados);

b) definir, documentar, aplicar normas y autorización para el despliegue de "software" desde el estado de desarrollo hasta el de producción;

c) probar cambios en sistemas y aplicaciones de producción en un entorno de prueba o de ensayo antes de aplicarlos a sistemas de producción (ver 8.29);

d) no realizar pruebas en entornos de producción, salvo en circunstancias definidas y aprobadas;

e) no ser accesibles desde sistemas de producción en que no se requiera que los compiladores, editores y otras herramientas de desarrollo o programas de utilidad;

f) mostrar etiquetas de identificación de entorno adecuadas en menús para reducir el riesgo de error;

g) no copiar información sensible en entornos de los sistemas de desarrollo y de prueba, a menos que se establezcan controles equivalentes para los sistemas de desarrollo y de prueba.

En todos los casos, los entornos de desarrollo y prueba se deberían proteger considerando:

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 de “software”;

c) control de acceso a entornos;

d) supervisión de cambios en el entorno y código almacenado en él;

e) supervisión segura de entornos;

f) realización de copias de seguridad de entornos.

Una sola persona no debería tener la capacidad de realizar cambios tanto en desarrollo como en producción sin una revisión y aprobación previas. Esto se puede lograr, por ejemplo, mediante segregación de derechos de acceso o a través de reglas supervisadas. En situaciones excepcionales, se deberían aplicar medidas adicionales, como registro detallado y supervisión en tiempo real, para detectar cambios no autorizados y actuar en consecuencia.

Otra información

Sin medidas y procedimientos adecuados, el acceso de desarrolladores y probadores a sistemas de producción puede introducir riesgos importantes (por ejemplo, modificación no deseada de archivos o del entorno de sistema, el fallo de sistema, ejecución de código no autorizado y no probado en los sistemas de producción, divulgación de datos confidenciales, problemas de integridad y disponibilidad de los datos). Es necesario mantener un entorno conocido y estable en el que realizar pruebas significativas y evitar acceso inapropiado de desarrolladores al entorno de producción.

Las medidas y procedimientos incluyen el diseño cuidadoso de funciones junto con la aplicación de requisitos de separación de funciones e implantación de procesos de supervisión adecuados.

El personal de desarrollo y pruebas también supone una amenaza para la confidencialidad de la información de producción. Actividades de desarrollo y prueba pueden provocar cambios involuntarios en “software” o información si comparten el mismo entorno informático. Por lo tanto, es conveniente separar entornos de desarrollo, pruebas y producción para reducir el riesgo de cambios accidentales o de acceso no autorizado al “software” de producción y a datos empresariales (ver 8.33 para la protección de información de pruebas).

En algunos casos, la distinción entre entornos de desarrollo, prueba y producción se puede difuminar deliberadamente y las pruebas se pueden llevar a cabo en un entorno de desarrollo o mediante despliegues controlados a usuarios o servidores en vivo (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, las pruebas de producto se pueden realizar mediante uso en vivo de producto dentro de la organización. Además, para reducir el tiempo de inactividad de los despliegues en vivo, se pueden apoyar dos entornos de producción idénticos en que solo uno está en vivo en un momento dado.

Son necesarios procesos de apoyo para el uso de datos de producción en entornos de desarrollo y pruebas (8.33).

Las organizaciones también pueden tener en cuenta las orientaciones proporcionadas en esta sección para entornos de formación cuando realicen la formación de los usuarios finales.

8.32 Gestión de cambio

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_ netdeberíawork_security	#Protection

Control

Los cambios en instalaciones de procesamiento de información y en sistemas de información deberían estar sujetos a procedimientos de gestión de cambios.

Propósito

Para preservar seguridad de la información al ejecutar los cambios.

Guía

La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debería seguir unas normas acordadas y un proceso formal de documentación, especificación, pruebas, control de calidad e implementación gestionada. Se deberían establecer responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios se deberían documentar y aplicar para garantizar la confidencialidad, integridad y disponibilidad de información en instalaciones de procesamiento de información y sistemas de información, para todo el ciclo de vida de desarrollo de sistema, desde primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores

Siempre que sea posible, los procedimientos de control de cambios para la infraestructura y el “software” de ICT deberían estar integrados.

Los procedimientos de control de cambios deberían incluir:

a) planificación y evaluación de impacto potencial de cambios teniendo en cuenta todas las dependencias;

b) autorización de cambios;

c) comunicación de cambios a las partes interesadas;

d) pruebas y aceptación de pruebas de cambios (ver 8.29);

e) aplicación de cambios, incluyendo planes de despliegue;

f) consideración de emergencias y contingencias, incluyendo procedimientos de "fall-back[17]";

g) mantención de un registro de los cambios que incluya todo lo anterior;

h) garantías de que la documentación operativa (ver 5.37) y procedimientos de los usuarios se modifiquen según sea necesario para seguir siendo adecuados;

i) garantías de que los planes de continuidad de ICT y procedimientos de respuesta y recuperación (ver 5.30) se modifiquen según sea necesario para seguir siendo adecuados.

Otra información

El control inadecuado de los cambios en las instalaciones de procesamiento de información y en sistemas de información es una causa común de fallos de sistema o de seguridad. Cambios en entorno de producción, especialmente cuando se transfieren programas informáticos de entorno de desarrollo al operativo, pueden repercutir en integridad y disponibilidad de aplicaciones.

Los cambios en "software" pueden afectar al entorno de producción y viceversa.

Las buenas prácticas incluyen la prueba de componentes de ICT en un entorno separado de entornos de producción y desarrollo (ver 8.31). Esto proporciona un medio para tener control sobre el nuevo "software" y permite una protección adicional de información operativa que se usa para las pruebas. Esto debería incluir parches, paquetes de servicio y otras actualizaciones.

El entorno de producción incluye sistemas operativos, bases de datos y plataformas de "middleware[18]". El control se debería aplicar para cambios de aplicaciones e infraestructuras.

8.33 Información de prueba

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

Control

La información de las pruebas se debería seleccionar, proteger y gestionar adecuadamente.

Propósito

Garantizar la pertinencia de pruebas y protección de información operativa usada para las mismas.

17 Del inglés fall-back: *operación degradada.*

18 Del inglés: *soporte intermedio*.

Guía

Se debería seleccionar la información de pruebas para garantizar fiabilidad de resultados de pruebas y confidencialidad de información operativa pertinente. Información sensible (incluyendo información de identificación personal) no se debería copiar en entornos de desarrollo y pruebas (ver 8.31).

Las siguientes directrices se deberían aplicar para proteger las copias de la información operativa, cuando se usan con fines de prueba, tanto si el entorno de prueba se construye internamente como en un servicio en la nube:

a) aplicar a entornos de prueba de los mismos procedimientos de control de acceso que se aplican a entornos operativos;

b) tener una autorización independiente cada vez que se copie información operativa a un entorno de pruebas;

c) registrar copia y uso de información operativa para proporcionar una pista de auditoría;

d) proteger información sensible mediante su eliminación o enmascaramiento (ver 8.11) si se usa para pruebas;

e) eliminar adecuadamente (ver 8.10) información operativa de un entorno de prueba inmediatamente después de que se completó la prueba para evitar uso no autorizado de información de prueba.

La información de las pruebas se debería almacenar de forma segura (para evitar su manipulación, que de otro modo podría dar lugar a resultados no válidos) y usar únicamente con 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 sistemas de información durante pruebas de auditoría

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

Control

Las pruebas de auditoría y otras actividades de garantía que impliquen evaluación de sistemas operativos se deberían planificar y acordar entre el encargado de pruebas y dirección correspondiente.

Propósito

Minimizar impacto de auditorías y otras actividades de garantía en los sistemas operativos y los procesos empresariales.

Guía

Se deberían observar las siguientes directrices:

a) acordar solicitudes de auditoría para el acceso a los sistemas y datos con la dirección correspondiente;

b) acordar y controlar alcance de pruebas técnicas de auditoría;

c) limitar pruebas de auditoría al acceso de solo lectura al “software” y a datos. Si no se dispone de acceso de solo lectura para obtener información necesaria, ejecutar prueba por un administrador experimentado que tenga derechos de acceso necesarios en nombre del auditor;

d) establecer y verificar requisitos de seguridad, si se concede acceso, (por ejemplo, antivirus y parches) de dispositivos usados para acceder a sistemas (por ejemplo, ordenadores portátiles o tabletas) antes de permitir el acceso;

e) permitir únicamente acceso a copias aisladas de los archivos de sistema que no sean de solo lectura, borrándolas una vez finalizada la auditoría, o dándoles protección adecuada si existe obligación de conservar dichos archivos en virtud de requisitos de documentación de auditoría;

f) identificar y acordar solicitudes de tratamiento especial o adicional, como ejecución de herramientas de auditoría;

g) realizar pruebas de auditoría que puedan afectar a la disponibilidad de sistema fuera del horario laboral;

h) supervisar y registrar todos los accesos con fines de auditoría y prueba.

Otra información

Las pruebas de auditoría y otras actividades de garantía también se pueden realizar en sistemas de desarrollo y de prueba, en que dichas pruebas pueden afectar, por ejemplo, a la integridad del código o provocar la divulgación de cualquier información sensible que se encuentre en dichos entornos.

Anexo A
(informativo)

Uso de atributos

A.1 Generalidades

Este anexo proporciona una tabla para demostrar el uso de los atributos como forma de crear diferentes vistas de controles. Los cinco ejemplos de atributos son (ver 4.2):

a) Tipos de control (#Preventive, #Detective, #Corrective)

b) Propiedades de seguridad de la información (#Confidentiality, #Integrity, #Availability)

c) Conceptos de ciberseguridad (#Identify, #Protect, #Detect, #Respond, #Recover)

d) Capacidades operativas (#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance)

e) Ámbitos de seguridad (#Governance_and_Ecosystem, #Protection, #Defence, #Resilience)

La Tabla A.1 contiene una matriz de todos los controles de esta norma con los valores de sus atributos.

El filtro u ordenación de la matriz se puede lograr usando una herramienta como una simple hoja de cálculo o una base de datos, que puede incluir más información como texto de control, orientación, guía específica de la organización o atributos (ver A.2).

Tabla A.1 – Matriz de controles y valores de atributos

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.1	Políticas de seguridad de la información	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosystem #Resilience
5.2	Funciones y responsabilidades en materia de seguridad de la información	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_ Ecosystem #Protection #Resilience

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.3	Segregación de deberes	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_ access_ management	#Governance_ and_Ecosystem
5.4	Responsabilidades de gestión	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosystem
5.5	Contacto con autoridades	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contacto con grupos de interés especiales	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Inteligencia sobre amenazas	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_ vulnerability_ management	#Defence #Resilience
5.8	Seguridad de la información en la gestión de proyectos	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_ and_Ecosystem #Protection
5.9	Inventario de información y otros activos asociados	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_ management	#Governance_ and_Ecosystem #Protection
5.10	Uso aceptable de información y otros activos asociados	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection	#Governance_ and_Ecosystem #Protection
5.11	Retorno de activos	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management	#Protection
5.12	Clasificación de información	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_ protection	#Protection #Defence
5.13	Etiquetado de información	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection
5.14	Transferencia de información	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection	#Protection

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.15	Control de acceso	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
5.16	Gestión de identidad	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
5.17	Información de autentificación	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
5.18	Derechos de acceso	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
5.20	Abordar seguridad de la información en acuerdos con proveedores	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
5.21	Gestión de seguridad de la información en la cadena de suministro de ICT	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
5.22	Monitoreo, revisión y gestión de cambios de los servicios de los proveedores	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_ relationships_ security #Information_ security_ assurance	#Governance_ and_Ecosystem #Protection #Defence
5.23	Seguridad de la información para uso de servicios en la nube	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
5.24	Planificación y preparación de gestión de incidentes de seguridad de la información	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_ security_event_ management	#Defence
5.25	Evaluación y decisión sobre eventos de seguridad de la información	#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event_ management	#Defence

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.26	Respuesta a incidentes de seguridad de la información	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_ security_event_ management	#Defence
5.27	Aprender de incidentes de seguridad de la información	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ security_event_ management	#Defence
5.28	Recogida de pruebas	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event_ management	#Defence
5.29	Seguridad de la información durante la interrupción	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	Preparación de ICT para la continuidad de la actividad	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.31	Requisitos legales, reglamentarios y contractuales	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosystem #Protection
5.32	Derechos de propiedad intelectual	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosystem
5.33	Protección de registros	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Asset_ management #Information_ protection	#Defence
5.34	Privacidad y protección de información personal	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ protection #Legal_and_ compliance	#Protection
5.35	Revisión independiente de seguridad de la información	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_ security_ assurance	#Governance_ and_Ecosystem

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Information_ security_ assurance	#Governance_ and_Ecosystem
5.37	Procedimientos operativos documentados	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_ management #Physical_ security #System_and_ network_security #Application_ security #Secure_ configuration #Identity_ and_access_ management #Threat_and_ vulnerability_ management #Continuity #Information_ security_event_ management	#Governance_ and_Ecosystem #Protection #Defence
6.1	Cribado	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_ resource_security	#Governance_ and_Ecosystem
6.2	Condiciones de empleo	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_ resource_security	#Governance_ and_Ecosystem
6.3	Sensibilización, educación y formación en materia de seguridad de la información	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_ resource_security	#Governance_ and_Ecosystem
6.4	Disciplina proceso	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_ resource_security	#Governance_ and_Ecosystem
6.5	Responsabilidades tras cese o cambio de empleo	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_ resource_security #Asset_ management	#Governance_ and_Ecosystem

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
6.6	Confidencialidad o de no divulgación de acuerdos	#Preventive	#Confidentiality	#Protect	#Human_ resource_security #Information_ protection #Supplier_ relationships	#Governance_ and_Ecosystem
6.7	Trabajo a distancia	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection #Physical_ security #System_and_ network_security	#Protection
6.8	Informes de eventos de seguridad de la información	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_ security_event_ management	#Defence
7.1	Perímetros de seguridad física	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.2	Entrada física	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Identity_ and_Access_ Management	#Protection
7.3	Asegurar oficinas, salas e instalaciones	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.4	Vigilancia de seguridad física	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_ security	#Protection #Defence
7.5	Protección contra amenazas físicas y medioambientales	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.6	Trabajar en zonas seguras	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security	#Protection
7.7	Escritorio y pantalla despejados	#Preventive	#Confidentiality	#Protect	#Physical_ security	#Protection

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
7.8	Ubicación y protección de los equipos	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.9	Seguridad de activos fuera de las instalaciones	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.10	Medios de almacenamiento	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection
7.11	Servicios públicos de apoyo	#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_ security	#Protection
7.12	Seguridad del cableado	#Preventive	#Confidentiality #Availability	#Protect	#Physical_ security	#Protection
7.13	Mantenimiento de equipos	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_ security #Asset_ management	#Protection #Resilience
7.14	Eliminación segura o reutilización de equipos	#Preventive	#Confidentiality	#Protect	#Physical_ security #Asset_ management	#Protection
8.1	Dispositivos terminales del usuario	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_ management #Information_ protection	#Protection
8.2	Derechos de acceso privilegiados	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
8.3	Restricción de acceso a información	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
8.4	Acceso al código fuente	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_access_ management #Application_ security #Secure_ configuration	#Protection
8.5	Autenticación segura	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_ management	#Protection
8.6	Gestión de capacidad	#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_ and_Ecosystem #Protection

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.7	Protección contra “malware”	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_security #Information_ protection	#Protection #Defence
8.8	Gestión de las vulnerabilidades técnicas	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Protection #Defence
8.9	Gestión de la configuración	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration	#Protection
8.10	Información borrado	#Preventive	#Confidentiality	#Protect	#Information_ protection #Legal_and_ compliance	#Protection
8.11	Enmascaramiento de datos	#Preventive	#Confidentiality	#Protect	#Information_ protection	#Protection
8.12	Fuga de datos prevención	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_ protection	#Protection #Defence
8.13	Información de respaldo	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.14	Redundancia de las instalaciones de tratamiento de la información	#Preventive	#Availability	#Protect	#Continuity #Asset_ management	#Protection #Resilience
8.15	Registro	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_ security_event_ management	#Protection #Defence
8.16	Actividades de monitoreo	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event_ management	#Defence
8.17	Sincronización de relojes	#Detective	#Integrity	#Protect #Detect	#Information_ security_event_ management	#Protection #Defence
8.18	Uso de programas de servicios públicos privilegiados	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security #Secure_ configuration #Application_ security	#Protection

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (continuación)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.19	Instalación de software en sistemas operativos	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration #Application_ security	#Protection
8.20	Redes de seguridad	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_security	#Protection
8.21	Seguridad de servicios de red	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection
8.22	Segregación de redes	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection
8.23	Filtrado Web	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security	#Protection
8.24	Uso de criptografía	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_ configuration	#Protection
8.25	Ciclo de vida de desarrollo seguro	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection
8.26	Requisitos de seguridad de las aplicaciones	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection #Defence
8.27	Arquitectura de sistemas seguros y principios de ingeniería	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection
8.28	Codificación segura	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection
8.29	Pruebas de seguridad en desarrollo y aceptación	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_ security #Information_ security_ assurance #System_and_ network_security	#Protection

(continúa)

Tabla A.1 – Matriz de controles y valores de atributos (conclusión)

ISO/ IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.30	Desarrollo subcontratado	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_ network_security #Application_ security #Supplier_ relationships_ security	#Governance_ and_Ecosystem #Protection
8.31	Separación de entornos de desarrollo, prueba y producción	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection
8.32	Gestión del cambio	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_ security #System_and_ network_security	#Protection
8.33	Información de la prueba	#Preventive	#Confidentiality #Integrity	#Protect	#Information_ protection	#Protection
8.34	Protección de los sistemas de información durante las pruebas de auditoría	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_ network_security #Information_ protection	#Governance_ and_Ecosystem #Protection

La Tabla A.2 muestra un ejemplo de cómo crear una vista filtrando por un valor de atributo concreto, en este caso #Corrective.

Tabla A.2 – Vista de los controles de #Corrective

ISO/IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.5	Contacto con las autoridades	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contacto con grupos de interés especiales	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Inteligencia sobre amenazas	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_ vulnerability_ management	#Defence #Resilience

(continúa)

Tabla A.2 – Vista de los controles de #Corrective (continuación)

ISO/IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.26	Respuesta a los incidentes de seguridad de la información	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
5.28	Recogida de pruebas	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
5.29	Seguridad de la información durante la interrupción	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	Preparación de ICT para la continuidad de la actividad	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.35	Revisión independiente de seguridad de la información	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
5.37	Procedimientos operativos documentados	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

(continúa)

Tabla A.2 – Vista de los controles de #Corrective (conclusión)

ISO/IEC 27002 controlar identificador	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
6.4	Disciplina proceso	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_ resource_security	#Governance_ and_Ecosystem
8.7	Protección contra “malware”	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_ network_security #Information_ protection	#Protection #Defence
8.13	Información de respaldo	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.16	Actividades de monitoreo	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_ security_event_ management	#Defence

A.2 Visión organizativa

Dado que los atributos se usan para crear diferentes puntos de vista de los controles, las organizaciones pueden descartar los ejemplos de atributos propuestos en esta norma 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 las organizaciones, ya que estas pueden tener diferentes puntos de vista sobre uso o aplicabilidad del control o de valores asociados al atributo (en que los valores son específicos del contexto de la organización). El primer paso es entender por qué es deseable un atributo específico de la organización. Por ejemplo, si una organización construyó sus planes de tratamiento de riesgos [ver ISO/IEC 27001:2013, 6.1.3 e)] basándose en eventos, puede desear asociar un atributo de escenario de riesgo a cada control de esta norma.

El beneficio de dicho atributo es agilizar el proceso de cumplimiento del requisito de la norma 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 “necesary”), con estas en la norma ISO/IEC 27001:2013, Anexo A (que se emiten a partir de esta norma) para asegurar que no se pasó por alto ningún control necesario.

Una vez conocidos el objetivo y 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 en instalaciones de la organización;

3) fuerza mayor, vandalismo y terrorismo;

4) fallo 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 realizar asignando identificadores a cada evento (por ejemplo, E1, E2, ..., E9).

El tercer paso es copiar los identificadores y nombres de los controles de esta norma en una hoja de cálculo o en una base de datos y asociar valores de atributos a cada control, recordando que cada control puede tener más de un valor de atributo.

El último paso es ordenar la hoja de cálculo o consultar la base de datos para extraer la información necesaria. Otros ejemplos de atributos organizativos (y posibles valores) son:

a) madurez (valores de las normas ISO/IEC 33000 u otros modelos de madurez);

b) estado de aplicación (por hacer, en curso, parcialmente aplicado, totalmente aplicado);

c) prioridad (1, 2, 3, otro);

d) áreas organizativas implicadas (seguridad, ICT, recursos humanos, alta dirección, otro);

e) eventos;

f) activos implicados;

g) construcción y ejecución, para diferenciar los controles utilizados en las diferentes etapas del ciclo de vida del servicio;

h) otros marcos con los que la organización trabaja o de los que puede hacer la transición

Anexo B
(informativo)

Relación entre la norma ISO/IEC 27002:2022 (esta norma) y la norma ISO/IEC 27002:2013

El propósito de este anexo es proporcionar compatibilidad con la norma ISO/IEC 27002:2013 para las organizaciones que actualmente están usando esa norma y ahora desean hacer la transición a esta edición.

La Tabla B.1 proporciona la relación de los controles especificados en las cláusula 5 a 8 con la norma ISO/IEC 27002:2013.

Tabla B.1 – Relación entre controles de esta norma y controles de la norma ISO/IEC 27002:2013

ISO/IEC 27002:2022 controlar identificador	ISO/IEC 27002:2013 controlar identificador	Nombre del control
5.1	05.1.1, 05.1.2	Políticas de seguridad de la información
5.2	06.1.1	Funciones y responsabilidades en materia de seguridad de la información
5.3	06.1.2	Segregación de funciones
5.4	07.2.1	Responsabilidades de gestión
5.5	06.1.3	Contacto con las autoridades
5.6	06.1.4	Contacto con grupos de interés especiales
5.7	Nuevo	Inteligencia sobre 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 la 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 la identidad
5.17	09.2.4, 09.3.1, 09.4.3	Información de autentificación
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso

(continúa)

Tabla B.1 – Relación entre controles de esta norma y controles de la norma ISO/IEC 27002:2013
(continuación)

ISO/IEC 27002:2022 controlar identificador	ISO/IEC 27002:2013 controlar identificador	Nombre del control
5.19	15.1.1	Seguridad de la información en las relaciones con los proveedores
5.20	15.1.2	Abordar seguridad de la información en los acuerdos con los proveedores
5.21	15.1.3	Gestión de seguridad de la información en la cadena de suministro de ICT
5.22	15.2.1, 15.2.2	Monitoreo, revisión y gestión de cambios de los servicios de los 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
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de incidentes de seguridad de la información
5.28	16.1.7	Recogida de pruebas
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de ICT para la continuidad de la actividad
5.31	18.1.1, 18.1.5	Requisitos legales, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual
5.33	18.1.3	Protección de los registros
5.34	18.1.4	Privacidad y protección de información personal
5.35	18.2.1	Revisión independiente de seguridad de la información
5.36	18.2.2, 18.2.3	Cumplimiento de políticas, reglas y normas de seguridad de la información
5.37	12.1.1	Procedimientos operativos documentados
6.1	07.1.1	Cribado
6.2	07.1.2	Condiciones de empleo
6.3	07.2.2	Sensibilización, educación y formación en materia de seguridad de la información
6.4	07.2.3	Proceso disciplinario
6.5	07.3.1	Responsabilidades tras cese o cambio de empleo
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Trabajo a distancia
6.8	16.1.2, 16.1.3	Informes de eventos de seguridad de la información
7.1	11.1.1	Perímetros de seguridad física
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Asegurar las oficinas, salas e instalaciones
7.4	Nuevo	Vigilancia de la seguridad física

(continúa)

Tabla B.1 – Relación entre controles de esta norma y controles de la norma ISO/IEC 27002:2013

(continuación)

ISO/IEC 27002:2022 controlar identificador	ISO/IEC 27002:2013 controlar identificador	Nombre del control
7.5	11.1.4	Protección contra amenazas físicas y medioambientales
7.6	11.1.5	Trabajar en zonas seguras
7.7	11.2.9	Escritorio y pantalla despejados
7.8	11.2.1	Ubicación y protección de los 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	Servicios públicos de apoyo
7.12	11.2.3	Seguridad del cableado
7.13	11.2.4	Mantenimiento de equipos
7.14	11.2.7	Eliminación segura o reutilización de los equipos
8.1	06.2.1, 11.2.8	Dispositivos terminales del usuario
8.2	09.2.3	Derechos de acceso privilegiados
8.3	09.4.1	Restricción de acceso a 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”
8.8	12.6.1, 18.2.3	Gestión de vulnerabilidades técnicas
8.9	Nuevo	Gestión de configuración
8.10	Nuevo	Eliminación de información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de la fuga de datos
8.13	12.3.1	Información de respaldo
8.14	17.2.1	Redundancia de las instalaciones de tratamiento de la información
8.15	12.4.1, 12.4.2, 12.4.3	Registro
8.16	Nuevo	Actividades de monitoreo
8.17	12.4.4	Sincronización del 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 de las redes

(continúa)

Tabla B.1 – Relación entre controles de esta norma y controles de la norma ISO/IEC 27002:2013

(conclusión)

ISO/IEC 27002:2022 controlar identificador	ISO/IEC 27002:2013 controlar identificador	Nombre del control
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 la criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de aplicaciones
8.27	14.2.5	Arquitectura de sistemas seguros y principios de ingeniería
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 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 la prueba
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

La Tabla B.2 proporciona la relación entre controles especificados en la norma ISO/IEC 27002:2013 con esta norma.

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
5		Políticas de seguridad de la información
5.1		Dirección de la gestión de seguridad de la información
5.1.1	5.1	Políticas de seguridad de la información
5.1.2	5.1	Revisión de políticas de seguridad de la información
6		La organización de seguridad de la información
6.1		La organización interna
6.1.1	5.2	Funciones y responsabilidades en materia de seguridad de la información
6.1.2	5.3	Segregación de funciones
6.1.3	5.5	Contacto con autoridades
6.1.4	5.6	Contacto con grupos de interés especiales
6.1.5	5.8	Seguridad de la información en gestión de proyectos

(continúa)

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma (continuación)

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
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	Cribado
7.1.2	6.2	Condiciones de empleo
7.2		Durante el empleo
7.2.1	5.4	Responsabilidades de gestión
7.2.2	6.3	Sensibilización, educación y formación en materia de seguridad de información
7.2.3	6.4	Proceso disciplinario
7.3		Cese y cambio de empleo
7.3.1	6.5	Cese o cambio de responsabilidades laborales
8		Gestión de activos
8.1		Responsabilidad de 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 información
8.2.1	5.12	Clasificación de información
8.2.2	5.13	Etiquetado de información
8.2.3	5.10	Manejo de activos
8.3		Manejo de medios de comunicación
8.3.1	7.10	Gestión de soportes extraíbles
8.3.2	7.10	Eliminación de soportes
8.3.3	7.10	Transferencia de medios físicos
9		Control de acceso
9.1		Requisitos empresariales del 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 los usuarios
9.2.1	5.16	Registro y baja de usuarios

(continúa)

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma (continuación)

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
9.2.2	5.18	Provisión de acceso a los usuarios
9.2.3	8.2	Gestión de derechos de acceso privilegiados
9.2.4	5.17	Gestión de la información secreta de autentificación de los usuarios
9.2.5	5.18	Revisión de derechos de acceso de usuarios
9.2.6	5.18	Supresión o ajuste de derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de información secreta de autenticación
9.4		Control de acceso al sistema y a aplicaciones
9.4.1	8.3	Restricción del acceso a 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 de uso de controles criptográficos
10.1.2	8.24	Gestión de claves
11		Seguridad física y medioambiental
11.1		Zonas seguras
11.1.1	7.1	Perímetro de seguridad física
11.1.2	7.2	Controles físicos de entrada
11.1.3	7.3	Asegurar las oficinas, salas e instalaciones
11.1.4	7.5	Protección contra las amenazas externas y medioambientales
11.1.5	7.6	Trabajar en zonas seguras
11.1.6	7.2	Zonas de entrega y carga
11.2		Equipo
11.2.1	7.8	Ubicación y protección de equipos
11.2.2	7.11	Servicios públicos de apoyo
11.2.3	7.12	Seguridad del cableado
11.2.4	7.13	Mantenimiento de los equipos
11.2.5	7.10	Retirada de activos
11.2.6	7.9	Seguridad de equipos y activos fuera de instalaciones
11.2.7	7.14	Eliminación segura o reutilización de los equipos

(continúa)

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma (continuación)

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de mesas y pantallas despejadas
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, prueba y operación
12.2		Protección contra el “malware”
12.2.1	8.7	Controles contra el “malware”
12.3		Copia de seguridad
12.3.1	8.13	Información de respaldo
12.4		Registro y control
12.4.1	8.15	Registro de eventos
12.4.2	8.15	Protección de la información de los registros
12.4.3	8.15	Registros del administrador y del operador
12.4.4	8.17	Sincronización del reloj
12.5		Control del “software” operativo
12.5.1	8.19	Instalación de “software” en sistemas operativos
12.6		Gestión de vulnerabilidad técnica
12.6.1	8.8	Gestión de vulnerabilidades técnicas
12.6.2	8.19	Restricciones a la instalación de “software”
12.7		Consideraciones sobre la auditoría de los sistemas de información
12.7.1	8.34	Controles de auditoría de los sistemas de información
13		Seguridad de las comunicaciones
13.1		Instalaciones de gestión de la seguridad de la red.
13.1.1	8.20	Controles de red
13.1.2	8.21	Seguridad de servicios de red
13.1.3	8.22	Segregación en las redes
13.2		Transferencia de información
13.2.1	5.14	Políticas y procedimientos de transferencia de información
13.2.2	5.14	Acuerdos sobre la transferencia de información
13.2.3	5.14	Mensajería electrónica

(continúa)

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma (continuación)

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
13.2.4	6.6	Acuerdos de confidencialidad o no divulgación
14		Adquisición, desarrollo y mantenimiento de sistema
14.1		Requisitos de seguridad de los sistemas de información
14.1.1	5.8	Análisis y especificación de los requisitos de seguridad de la información
14.1.2	8.26	Seguridad de los servicios de aplicaciones en redes públicas
14.1.3	8.26	Protección de las transacciones de los servicios de aplicación
14.2		Seguridad en los procesos de desarrollo y apoyo
14.2.1	8.25	Política de desarrollo segura
14.2.2	8.32	Procedimientos de control de cambios de sistema
14.2.3	8.32	Revisión técnica de las aplicaciones tras los cambios en la 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 de sistema
14.2.9	8.29	Pruebas de aceptación de sistema
14.3		Datos de la prueba
14.3.1	8.33	Protección de los datos de las pruebas
15		Relaciones con los proveedores
15.1		Seguridad de la información en relaciones con proveedores
15.1.1	5.19	Política de seguridad de la información para las relaciones con los proveedores
15.1.2	5.20	Seguridad en acuerdos con proveedores
15.1.3	5.21	Cadena de suministro de tecnologías de información y comunicación
15.2		Gestión de prestación de servicios de proveedores
15.2.1	5.22	Monitoreo y revisión de servicios de proveedores
15.2.2	5.22	Gestión de cambios en servicios de proveedores
16		Gestión de incidentes de seguridad de la información
16.1		Gestión de incidentes y mejoras en seguridad de la información
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Notificación de eventos de seguridad de la información
16.1.3	6.8	Informar de puntos débiles de 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

(continúa)

Tabla B.2 – Relación entre controles en ISO/IEC 27002:2013 y controles con esta norma (conclusión)

ISO/IEC 27002:2013 controlar identificador	ISO/IEC 27002:2022 controlar identificador	Nombre de control según ISO/IEC 27002:2013
16.1.6	5.27	Aprender de los incidentes de seguridad de la información
16.1.7	5.28	Recogida de pruebas
17		Aspectos de seguridad de la información en gestión de continuidad de actividad
17.1		Continuidad de seguridad de la información
17.1.1	5.29	Planificación de la continuidad de seguridad de la información
17.1.2	5.29	Implementación de la continuidad de seguridad de la información
17.1.3	5.29	Verificar, revisar y evaluar la continuidad de seguridad de la información
17.2		Despidos
17.2.1	8.14	Disponibilidad de instalaciones para el tratamiento de información
18		Cumplimiento
18.1		Cumplimiento de requisitos legales y contractuales
18.1.1	5.31	Identificación de legislación aplicable y de requisitos contractuales
18.1.2	5.32	Derechos de propiedad intelectual
18.1.3	5.33	Protección de los registros
18.1.4	5.34	Privacidad y protección de información personal identificable
18.1.5	5.31	Regulación de los controles criptográficos
18.2		Revisiones de seguridad de la información
18.2.1	5.35	Revisión independiente de seguridad de la información
18.2.2	5.36	Cumplimiento de políticas y normas de seguridad
18.2.3	5.36, 8.8	Revisión de la conformidad técnica

Anexo C
(informativo)

Bibliografía

[1] ISO 9000, *Quality management systems - Fundamentals and vocabulary*.

[2] ISO 55001, *Asset management - Management systems - Requirements*.

[3] ISO/IEC 11770 (all parts), *Information security - Key management*.

[4] ISO/IEC 15408 (all parts), *Information technology - Security techniques - Evaluation criteria for IT security.*

[5] ISO 15489 (all parts), *Information and documentation - Records management*.

[6] ISO/IEC 17788, *Information technology - Cloud computing - Overview and vocabulary.*

[7] ISO/IEC 17789, *Information technology - Cloud computing - Reference architecture*.

[8] ISO/IEC 19086 (all parts), *Cloud computing - Service level agreement (SLA) framework.*

[9] ISO/IEC 19770 (all parts), *Information technology - IT asset management*.

[10] ISO/IEC 19941, *Information technology - Cloud computing - Interoperability and portability.*

[11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of Techniques.*

[12] ISO 21500, *Project, programme and portfolio management - Context and concepts*.

[13] ISO 21502, *Project, programme and portfolio management - Guidance on project management.*

[14] ISO 22301, *Security and resilience - Business continuity management systems - Requirements.*

[15] ISO 22313, *Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301.*

[16] ISO/TS 22317, *Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA*).

[17] ISO 22396, *Security and resilience - Community resilience - Guidelines for information Exchange between organizations*.

[18] ISO/IEC TS 23167, *Information technology - Cloud computing - Common technologies and Techniques.*

[19] ISO/IEC 23751, *Information technology - Cloud computing and distributed platforms - Data sharing agreement (DSA) framework.*

[20] ISO/IEC 24760 (all parts), *IT Security and Privacy - A framework for identity management.*

[21] ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems - Requirements.*

[22] ISO/IEC 27005, *Information technology - Security techniques - Information security risk Management.*

[23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing.*

[24] ISO/IEC TS 27008, *Information technology - Security techniques - Guidelines for the assessment of information security controls.*

[25] ISO/IEC 27011, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.*

[26] ISO/IEC TR 27016, *Information technology - Security techniques - Information security management - Organizational economics.*

[27] ISO/IEC 27017, *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[28] ISO/IEC 27018, *Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*

[29] ISO/IEC 27019, *Information technology - Security techniques - Information security controls for the energy utility industry.*

[30] ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.*

[31] ISO/IEC 27033 (all parts), *Information technology - Security techniques - Network security.*

[32] ISO/IEC 27034 (all parts), *Information technology - Application security.*

[33] ISO/IEC 27035 (all parts), *Information technology - Security techniques - Information security incident management.*

[34] ISO/IEC 27036 (all parts), *Information technology - Security techniques - Information security for supplier relationships.*

[35] ISO/IEC 27037, *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.*

[36] ISO/IEC 27040, *Information technology - Security techniques - Storage security.*

[37] ISO/IEC 27050 (all parts), *Information technology - Electronic Discovery.*

[38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection - Cybersecurity framework development guidelines.*

[39] ISO/IEC 27701, *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.*

[40] ISO 27799, *Health informatics - Information security management in health using ISO/IEC 27002.*

[41] ISO/IEC 29100, *Information technology - Security techniques - Privacy framework.*

[42] ISO/IEC 29115, *Information technology - Security techniques - Entity authentication assurance Framework.*

[43] ISO/IEC 29134, *Information technology - Security techniques - Guidelines for privacy impact assessment.*

[44] ISO/IEC 29146, *Information technology - Security techniques - A framework for Access management.*

[45] ISO/IEC 29147, *Information technology - Security techniques - Vulnerability disclosure.*

[46] ISO 30000, *Ships and marine technology - Ship recycling management systems - Specifications for management systems for safe and environmentally sound ship recycling facilities.*

[47] ISO/IEC 30111, *Information technology - Security techniques - Vulnerability handling processes.*

[48] ISO 31000:2018, *Risk management - Guidelines.*

[49] IEC 31010, *Risk management - Risk assessment techniques.*

[50] ISO/IEC 22123 (all parts), *Information technology - Cloud computing.*

[51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection - Guidelines on personally identifiable information deletion.*

[52] Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/.

[53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076.

[54] National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-37r2.

[55] Open Web Application Security Project (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/.

[56] Open Web Application Security Project (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at https://github.com/OWASP/DevGuide.

[57] National Institute of Standards and Technology (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-63b.

[58] OASIS, Structured Threat Information Expression. Available at https://www.oasis-open.org/standards#stix2.0.

[59] OASIS, Trusted Automated Exchange of Indicator Information. Available at https://www.oasis-open.org/standards#taxii2.0.

NOTA EXPLICATIVA NACIONAL

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO 9000	NCh-ISO 9000:2015	La Norma Chilena NCh-ISO 9000:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO 9000:2015.
ISO 55001	NCh-ISO55001:2014	La Norma Chilena NCh-ISO55001:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO 55001:2014.
ISO/IEC 11770 (all parts)	No hay	-
ISO/IEC 15408 (all parts)	NCh-ISO IEC 15408/1:2020	La Norma Chilena NCh-ISO IEC 15408/1:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 15408-1:2009.
ISO 15489 (all parts)	No hay	-
ISO/IEC 17788	NCh-ISO17788:2015	La Norma Chilena NCh-ISO17788:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 17788:2014.
ISO/IEC 17789	NCh-ISO17789:2015	La Norma Chilena NCh-ISO17789:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 17789:2014.
ISO/IEC 19086 (all parts)	NCh-ISO IEC 19086/3:2019	La Norma Chilena NCh-ISO IEC 19086/3:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 19086-3:2017.
ISO/IEC 19770 (all parts)	No hay	-
ISO/IEC 19941	No hay	-
ISO/IEC 20889	No hay	-
ISO 21500	NCh-ISO21500:2021	La Norma Chilena NCh-ISO21500:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO 21500:2021.

(continúa)

(continuación)

ISO 21502	NCh-ISO21502:2021	La Norma Chilena NCh-ISO21500:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO 21502:2020.
ISO 22301	NCh-ISO22301:2020	La Norma Chilena NCh-ISO22301:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO 22301:2019.
ISO 22313	NCh-ISO22313:2020	La Norma Chilena NCh-ISO22313:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO 22313:2020.
ISO/TS 22317	NCh-ISO TS22317:2016	La Norma Chilena NCh-ISO TS22317:2016 es una adopción idéntica de la versión en español de la Norma Internacional ISO/TS 22317:2015.
ISO 22396	NCh-ISO22396:2020	La Norma Chilena NCh-ISO22396:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO 22396:2020.
ISO/IEC TS 23167	No hay	-
ISO/IEC 23751	No hay	-
ISO/IEC 24760 (all parts)	No hay	-
ISO/IEC 27001:2013	NCh-ISO IEC 27001:2020	La Norma Chilena NCh-ISO IEC 27001:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27001:2013 y sus corrigendas, ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015.
ISO/IEC 27005	NCh-ISO IEC 27005:2020	La Norma Chilena NCh-ISO IEC 27005:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27005:2018.
ISO/IEC 27007	NCh-ISO IEC 27007:2020	La Norma Chilena NCh-ISO IEC 27007:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27007:2020.
ISO/IEC TS 27008	NCh-ISO/IEC TS27008:2019	La Norma Chilena NCh-ISO/IEC TS 27008:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC TS 27008:2019.
ISO/IEC 27011	NCh-ISO IEC 27011:2018	La Norma Chilena NCh-ISO IEC 27011:2018 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27011:2016.
ISO/IEC TR 27016	No hay	-
ISO/IEC 27017	NCh-ISO IEC 27017:2016	La Norma Chilena NCh-ISO IEC 27017:2016 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27017.
ISO/IEC 27018	NCh-ISO IEC 27018:2019	La Norma Chilena NCh-ISO IEC 27018:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27018:2019.

(continúa)

(continuación)

ISO/IEC 27019	NCh-ISO IEC 27019:2019	La Norma Chilena NCh-ISO IEC 27019:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27019:2017.
ISO/IEC 27031	NCh-ISO27031:2015	La Norma Chilena NCh-ISO27031:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27031:2011.
ISO/IEC 27033 (all parts)	NCh-ISO IEC 27033/1:2019	La Norma Chilena NCh-ISO IEC 27033/1:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27033-1:2015.
	NCh-ISO IEC 27033/2:2021	La Norma Chilena NCh-ISO IEC 27033/2:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27033-2:2012.
	NCh-ISO IEC 27033/3:2021	La Norma Chilena NCh-ISO IEC 27033/3:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27033-3:2010.
	NCh-ISO IEC 27033/4:2021	La Norma Chilena NCh-ISO IEC 27033/4:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27033-4:2014.
	NCh-ISO IEC 27033/5:2021	La Norma Chilena NCh-ISO IEC 27033/5:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27033-5:2013.
ISO/IEC 27034 (all parts)	NCh-ISO IEC 27034/1:2021	La Norma Chilena NCh-ISO IEC 27034/1:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27034-1:2011 y su corrigenda ISO/IEC 27034-1:2011/ Cor 1:2014.
	NCh-ISO IEC 27034/2:2021	La Norma Chilena NCh-ISO IEC 27034/2:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27034-2:2015.
	NCh-ISO IEC 27034/5:2021	La Norma Chilena NCh-ISO IEC 27034/5:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27034-5:2017.
	NCh-ISO IEC 27034/6:2021	La Norma Chilena NCh-ISO IEC 27034/6:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27034-6:2016.
	NCh-ISO IEC 27034/7:2021	La Norma Chilena NCh-ISO IEC 27034/7:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27034-7:2018.

(continúa)

(continuación)

ISO/IEC 27035 (all parts)	NCh-ISO IEC 27035/1:2018	La Norma Chilena NCh-ISO IEC 27035/1:2018 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27035-1:2016.
	NCh-ISO IEC 27035/2:2019	La Norma Chilena NCh-ISO IEC 27035/2:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27035-2:2016.
	NCh-ISO IEC 27035/3:2022	La Norma Chilena NCh-ISO IEC 27035/3:2022 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27035-3:2020.
ISO/IEC 27036 (all parts)	NCh-ISO IEC 27036/1:2022	La Norma Chilena NCh-ISO IEC 27036/1:2022 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27036-1:2021.
	NCh-ISO27036/2:2015	La Norma Chilena NCh-ISO27036/2:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27036-2:2014.
	NCh-ISO27036/3:2015	La Norma Chilena NCh-ISO27036/3:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27036-3:2013.
	NCh-ISO IEC 27036/4:2021	La Norma Chilena NCh-ISO IEC 27036/4:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27036-4:2016.
ISO/IEC 27037	NCh-ISO27037:2015	La Norma Chilena NCh-ISO27037:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27037:2012.
ISO/IEC 27040	NCh-ISO27040:2015	La Norma Chilena NCh-ISO27040:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27040:2015.
ISO/IEC 27050 (all parts)	No hay	-
ISO/IEC TS 27110	No hay	-
ISO/IEC 27701	NCh-ISO IEC 27701:2020	La Norma Chilena NCh-ISO IEC 27701:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27701:2019.
ISO 27799	NCh-ISO27799:2018	La Norma Chilena NCh-ISO27799:2018 es una adopción idéntica de la versión en español de la Norma Internacional ISO 27799:2016.
ISO/IEC 29100	No hay	-
ISO/IEC 29115	No hay	-
ISO/IEC 29134	No hay	-
ISO/IEC 29146	No hay	-
ISO/IEC 29147	NCh-ISO IEC 29147:2019	La Norma Chilena NCh-ISO IEC 29147:2019 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 29147:2018.

(continúa)

(conclusión)

ISO 30000	No hay	-
ISO/IEC 30111	NCh-ISO IEC 30111:2021	La Norma Chilena NCh-ISO IEC 30111:2021 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 30111:2019.
ISO 31000:2018	NCh-ISO31000:2018	Idéntica
IEC 31010	NCh-IEC31010:2020	La Norma Chilena NCh-IEC31010:2020 es una adopción idéntica de la versión en español de la Norma Internacional ISO 31010:2019.
ISO/IEC 22123 (all parts)	No hay	-
ISO/IEC 27555	No hay	-

Anexo D
(informativo)

Justificación de los cambios editoriales

Tabla D.1 – Cambios editoriales

Cláusula/subcláusula	Cambios editoriales	Justificación
En toda la norma	Se reemplaza “este documento” por “esta norma”.	De acuerdo con estructura de NCh2.
En toda la norma	Se reemplaza “esta Norma Internacional” por “esta norma”.	La norma es de alcance nacional.
1	Se reemplaza “Alcance” por “Alcance y campo de aplicación”.	De acuerdo con estructura de NCh2.
Anexo C	Se agrega Nota Explicativa Nacional.	Para detallar la equivalencia y el grado de correspondencia de las Normas Internacionales con las Normas Chilenas.
Anexo C	Se reemplaza “Bibliografía” por “Anexo C (informativo) Bibliografía”.	De acuerdo con estructura de NCh2.